Canad. J. Math. Vol. **56** (1), 2004 pp. 23–54

Ternary Diophantine Equations via Galois Representations and Modular Forms

Michael A. Bennett and Chris M. Skinner

Abstract. In this paper, we develop techniques for solving ternary Diophantine equations of the shape $Ax^n + By^n = Cz^2$, based upon the theory of Galois representations and modular forms. We subsequently utilize these methods to completely solve such equations for various choices of the parameters A, B and C. We conclude with an application of our results to certain classical polynomial-exponential equations, such as those of Ramanujan–Nagell type.

1 Introduction

A recent approach to ternary Diophantine equations, based upon techniques from the theory of Galois representations and modular forms (and motivated by ideas of Frey [23], Hellegouarch [25] and Serre [51]), has achieved spectacular success in the work of Wiles [55], proving Fermat's Last Theorem. Subsequently, variants of these methods have been applied by Darmon and Merel [19] and Kraus [30], [31] to cases of the generalized Fermat equation

$$x^p + y^q = z^r, \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

While it does not seem possible to fully deal with this equation by these techniques (but see Darmon [17]), a number of partial (or even complete) results are available in case $(p, q, r) = (p, p, 2)$ (see [19] for $p \geq 5$), $(p, q, r) = (p, p, 3)$ (see [19] for $p \geq 5$), $(3, 3, p)$ (see [30] for $3 \leq p < 10^4$), $(4, p, 4)$ (see [14] for $p \geq 4$), $(2, 4, p)$, $(5, 5, p)$ and $(7, 7, p)$ (see [22], [32] and [32], resp.). Further, this approach makes it feasible to treat more general equations of the shape

$$Ax^p + By^q = Cz^r, \tag{1.1}$$

with A, B and C fixed nonzero integers. If $(p, q, r) = (p, p, p)$, earlier results along these lines are due to Serre [51] for $A = B = 1, C = L^\alpha$ ($\alpha \geq 1$), with

$$L \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}, \quad L \neq p, \quad p \geq 11,$$

Kraus [29] for $ABC = 15$, Darmon and Merel [19] for $ABC = 2$, and Ribet [49] for $ABC = 2^\alpha$ with $\alpha \geq 2$.

Received by the editors April 30, 2002; revised October 3, 2003.
AMS subject classification: 11D41, 11F11, 11G05.

In this paper, we will restrict our attention to equation (1.1) in the case $p = q$ and $r = 2$; *i.e.*, to

$$Ax^n + By^n = Cz^2. \tag{1.2}$$

Our aims are twofold. Firstly, we wish to develop a catalogue of techniques for solving a (relatively broad) class of ternary Diophantine equations. Secondly, we will apply these methods to explicitly solve certain Fermat-type equations. Such results have immediate applications to a variety of polynomial-exponential equations, such as those of Ramanujan–Nagell type, as well as to other classical Diophantine problems, including the occurence of powers in products of integers in arithmetic progressions.

We will suppose, here and henceforth, that A, B and C are nonzero pairwise coprime integers. As various authors have noted, if n is odd and $a, b, c \in \mathbb{Z}$ satisfy $Aa^n + Bb^n = Cc$, then $(ac, bc, c^{\frac{n+1}{2}})$ is an integral solution to (1.2). With this in mind, we will consider only *primitive* solutions (a, b, c) to (1.2), where we suppose that aA, bB and cC are nonzero and pairwise coprime. We may weaken this hypothesis, at the cost of a certain amount of simplicity.

Our main results, from the viewpoint of Diophantine equations, are as follows.

Theorem 1.1 *If $n \geq 4$ is an integer and*

$$C \in \{1, 2, 3, 5, 6, 10, 11, 13, 17\},$$

then the equation

$$x^n + y^n = Cz^2$$

has no solutions in nonzero pairwise coprime integers (x, y, z) with, say, $x > y$, unless $(n, C) = (4, 17)$ or

$$(n, C, x, y, z) \in \{(5, 2, 3, -1, \pm 11), (5, 11, 3, 2, \pm 5), (4, 2, 1, -1, \pm 1)\}.$$

If $C = 1$ this is a result of Darmon and Merel [19]. Our current methods are unable to resolve the case $C = 7$. With further computation, we can extend Theorem 1.1 to include, for example, $C \in \{14, 15, 19\}$.

Theorem 1.2 *Suppose that $n \geq 7$ is prime. If*

$$(C, \alpha_0) \in \{(1, 2), (3, 2), (5, 6), (7, 4), (11, 2), (13, 2), (15, 6), (17, 6)\},$$

then the equation

$$x^n + 2^\alpha y^n = Cz^2$$

has no solutions in nonzero pairwise coprime integers (x, y, z) with $xy \neq \pm 1$ and integers $\alpha \geq \alpha_0$, unless, possibly, $n \leq C$ or $(C, \alpha, n) = (11, 3, 13)$.

We should mention that the proofs of the above two theorems require combinations of every technique we have currently available. It is this application of more traditional results in concert with our Proposition 4.4 that represents the main novelty of this paper.

When AB is divisible by an odd prime and $C = 1$ or 2, as it transpires, we are rather limited in the techniques we may apply. In the situation where $A = C = 1$ and $B = p^m$ for $m \in \mathbb{N}$ and $p \equiv 3, 5 \pmod 8$ prime, distinct from 3 or $k^2 + 1$ with $k \in \mathbb{N}$, Ivorra [27] has shown that equation (1.2) is insoluble in coprime integers (x, y, z), provided n is a suitably large prime, relative to p. Such a result follows from careful examination of elliptic curves with conductor $2^\alpha p$ possessing at least one rational 2-torsion point. For small p, this is included in the following:

Theorem 1.3 *Suppose that $n \geq 11$ is prime, A, B are coprime integers, α, β are nonnegative integers with $\beta \geq 1$. If*

$$AB \in \{2^\alpha 11^\beta, 2^\alpha 13^\beta, 2^\alpha 19^\beta, 2^\alpha 29^\beta, 2^\alpha 43^\beta, 2^\alpha 53^\beta, 2^\alpha 59^\beta, 2^\alpha 61^\beta, 2^\alpha 67^\beta\}$$

for $\alpha = 0$ or $\alpha \geq 3$, or if

$$AB \in \{2 \cdot 19^\beta, 4 \cdot 11^\beta, 4 \cdot 19^\beta, 4 \cdot 43^\beta, 4 \cdot 59^\beta, 4 \cdot 61^\beta, 4 \cdot 67^\beta\}$$

then the equation

$$Ax^n + By^n = z^2$$

has no solution in nonzero pairwise coprime integers (x, y, z), unless, possibly, $n|AB$ or we have AB, n and α as follows:

AB	n	α	AB	n	α
$2^\alpha 19^\beta$	11	1	$2^\alpha 61^\beta$	13	$0, 3$
$2^\alpha 43^\beta$	11	$0, 3, \geq 7$	$2^\alpha 61^\beta$	31	≥ 7
$2^\alpha 53^\beta$	11	$2, 4, 5$	$2^\alpha 67^\beta$	11	$0, 3, 6$
$2^\alpha 53^\beta$	17	$0, 3$	$2^\alpha 67^\beta$	13	$0, 3$
$2^\alpha 59^\beta$	11	≥ 7	$2^\alpha 67^\beta$	17	$0, 3, \geq 7$
$2^\alpha 59^\beta$	29	6			

Theorem 1.4 *Suppose that $n \geq 11$ is prime and α is a nonnegative integer. If $B \in \{5^\alpha, 11^\alpha, 13^\alpha\}$, then the equation*

$$x^n + By^n = 2z^2$$

has no solution in nonzero pairwise coprime integers (x, y, z), unless, possibly, $n|B$.

For even values of AB, we have:

Theorem 1.5 *Suppose that $n \geq 11$ is prime, A, B are coprime integers, α, β, γ, δ are nonnegative integers with $\alpha \geq 6$ and $AB = 2^\alpha p^\beta q^\gamma$, where*

$$(p,q) \in \{(3,31)\ (\beta \geq 1),\ (5,11)\ (\alpha \geq 7),\ (5,19), (5,23)\ (\beta \geq 1),$$
$$(7,19)\ (\gamma \geq 1),\ (11,13), (11,23)\ (\beta \geq 1),\ (11,29), (11,31)\ (\beta \geq 1),$$
$$(13,31)\ (\beta \geq 1),\ (19,23)\ (\beta \geq 1),\ (19,29), (29,31)\ (\beta \geq 1)\}.$$

Then the equation

$$Ax^n + By^n = z^2$$

has no solution in nonzero pairwise coprime integers (x, y, z), unless, possibly, $n|AB$ or we have AB, n and α as follows:

AB	n	α	AB	n	α
$2^\alpha 5^\beta 23^\gamma$	11	≥ 7	$2^\alpha 11^\beta 29^\gamma$	13	≥ 7
$2^\alpha 7^\beta 19^\gamma$	11	≥ 7	$2^\alpha 19^\beta 23^\gamma$	11	≥ 7
$2^\alpha 11^\beta 23^\gamma$	11	≥ 6	$2^\alpha 19^\beta 29^\gamma$	11	≥ 7

where β, γ and δ are positive integers.

Finally, restricting to odd values of the variables x, y:

Theorem 1.6 *Suppose that $n \geq 11$ is prime and that α is a nonnegative integer. If $B \in \{23^\alpha, 31^\alpha, 47^\alpha, 71^\alpha\}$, then the equation*

$$x^n + By^n = z^2$$

has no solution in nonzero pairwise coprime integers (x, y, z) with $xy \equiv 1 \mod 2$, unless, possibly, $n|B$.

We note that in a number of cases, we may extend the above theorems to include analogous results with $n = 7$. We have, for the most part, omitted these for the sake of concision.

2 Some Elliptic Curves

We begin by writing down some elliptic curves. We always assume that n is an odd prime, that (a, b, c) is an integral solution to (1.2) with aA, bB and cC pairwise coprime, and that C is squarefree. Without loss of generality, we may suppose we are in one of the following situations:

(i) $abABC \equiv 1 \pmod 2$ and $b \equiv -BC \pmod 4$.
(ii) $ab \equiv 1 \pmod 2$ and either $\mathrm{ord}_2(B) = 1$ or $\mathrm{ord}_2(C) = 1$.
(iii) $ab \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) = 2$ and $c \equiv -bB/4 \pmod 4$.
(iv) $ab \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) \in \{3, 4, 5\}$ and $c \equiv C \pmod 4$.
(v) $\mathrm{ord}_2(Bb^n) \geq 6$ and $c \equiv C \pmod 4$.

For instance, let us suppose that $abABC$ is odd. Then we necessarily have $c \equiv 0 \pmod 2$ and, since n is odd, $aA \equiv \pm 1 \pmod 4$ while $bB \equiv \mp 1 \pmod 4$. Renaming if necessary, we may assume $b \equiv -BC \pmod 4$, whereby we find ourselves in case (i). The other cases are achieved by similar reasoning; note that we are free to replace c by $-c$, if necessary.

In cases (i) and (ii), we will consider the curve

$$E_1(a,b,c): \ Y^2 = X^3 + 2cCX^2 + BCb^nX.$$

In cases (iii) and (iv), we will consider

$$E_2(a,b,c): \ Y^2 = X^3 + cCX^2 + \frac{BCb^n}{4}X,$$

and in case (v),

$$E_3(a,b,c): \ Y^2 + XY = X^3 + \frac{cC-1}{4}X^2 + \frac{BCb^n}{64}X.$$

These are all elliptic curves defined over $\mathbb{Q}$.

The following lemma summarizes some useful facts about these curves.

Lemma 2.1 *Let $i = 1, 2$ or 3.*

(a) *The discriminant $\Delta(E)$ of the curve $E = E_i(a,b,c)$ is given by*

$$\Delta(E) = 2^{\delta_i} C^3 B^2 A (ab^2)^n,$$

where

$$\delta_i = \begin{cases} 6 & \text{if } i = 1 \\ 0 & \text{if } i = 2 \\ -12 & \text{if } i = 3. \end{cases}$$

(b) *The conductor $N(E)$ of the curve $E = E_i(a,b,c)$ is given by*

$$N(E) = 2^{\alpha} C^2 \prod_{p \mid abAB} p,$$

where

$$\alpha = \begin{cases} 5 & \text{if } i = 1, \text{ case (i)} \\ 6 & \text{if } i = 1, \text{ case (ii)} \\ 1 & \text{if } i = 2, \text{ case (iii)}, \ \mathrm{ord}_2(B) = 2 \text{ and } b \equiv -BC/4 \pmod 4 \\ 2 & \text{if } i = 2, \text{ case (iii)}, \ \mathrm{ord}_2(B) = 2 \text{ and } b \equiv BC/4 \pmod 4 \\ 4 & \text{if } i = 2, \text{ case (iv) and } \mathrm{ord}_2(B) = 3 \\ 2 & \text{if } i = 2, \text{ case (iv) and } \mathrm{ord}_2(B) \in \{4, 5\} \\ -1 & \text{if } i = 3, \text{ case (v) and } \mathrm{ord}_2(Bb^n) = 6 \\ 0 & \text{if } i = 3, \text{ case (v) and } \mathrm{ord}_2(Bb^n) \geq 7. \end{cases}$$

In particular, E has multiplicative reduction at each odd prime p dividing $abAB$. Also, E has multiplicative reduction at 2 if $\mathrm{ord}_2(Bb^n) \geq 7$.

(c) *The curve $E_i(a,b,c)$ has a $\mathbb{Q}$-rational point of order 2.*
(d) *Suppose p is an odd prime dividing C. The curve $E_i(a,b,c)$ obtains good reduction over $\mathbb{Q}(\sqrt[4]{C})$ at all primes ideals dividing p. Over any quadratic field K, the curve $E_i(a,b,c)$ has bad reduction at all prime ideals dividing p.*

Proof Part (a) of this lemma is just a straightforward calculation using the well-known formula for the discriminant of an elliptic curve given by a Weierstrass equation [52, III, §7]. Part (b) follows from Tate's algorithm for computing the reduced fiber of a Neron model of $E_i(a,b,c)$ together with Ogg's formula for the conductor [53, IV, §9]. The computations are somewhat involved at the prime 2. The stated results follow most easily from combining Propositions 1 to 7 with Tableau IV of Papadopolous [46]. By way of example, in case (i), we find that $\mathrm{ord}_2\big(c_4(E)\big) = 4$, $\mathrm{ord}_2\big(c_6(E)\big) \geq 6$ and $\mathrm{ord}_2\big(\Delta(E)\big) = 6$ and so may apply Proposition 1 and Tableau IV of [46] to conclude that $\alpha = 5$. Part (c) follows from the fact that $(X,Y) = (0,0)$ is a $\mathbb{Q}$-rational point of order 2 on $E_i(a,b,c)$ for each choice of i (*cf.* [52, III, 2.3]).

To prove part (d), let p be an odd prime dividing C. Consider the elliptic curves

$$E_1' : U^2 = V^3 + 2c\sqrt{C}V^2 + Bb^nV,$$

$$E_2' : U^2 = V^3 + c\sqrt{C}V^2 + \frac{Bb^n}{4}V,$$

and

$$E_3' : U^2 = V^3 + \frac{c\sqrt{C}}{4}V^2 + \frac{Bb^n}{64}V,$$

defined over $\mathbb{Q}(\sqrt{C})$. Note that the coefficients of the defining equations are integral except possibly at prime ideals dividing 2 and that the discriminants of these curves are each a power of 2 times $AB^2(ab^2)^n$ and hence coprime to p. It follows that these curves have good reduction at each prime ideal of $\mathbb{Q}(\sqrt{C})$ (and hence of $\mathbb{Q}(\sqrt[4]{C})$) dividing p [52, VII, 5.1].

For $i = 1$ or 2, the substitution $Y = C^{3/4}U$, $X = C^{1/2}V$ yields an isomorphism over $\mathbb{Q}(\sqrt[4]{C})$ between $E_i(a,b,c)$ and E_i'. The substitution $Y = C^{3/4}U - \frac{1}{2}C^{1/2}V$, $X = C^{1/2}V$ yields an isomorphism over $\mathbb{Q}(\sqrt[4]{C})$ between $E_3(a,b,c)$ and E_3'. Combining this with the preceding observation on the reduction of the E_i''s at a prime ideal dividing p gives the first half of part (d).

For the second half of (d), observe that $E_i(a,b,c)$ having good reduction over the quadratic field $\mathbb{Q}(\sqrt{D})$ (D squarefree) at each prime ideal dividing p is equivalent to the $\mathbb{Q}(\sqrt{D})$-quadratic twist of $E_i(a,b,c)$ having good reduction at p. The substitutions in [52, X, 2.4] yield a Weierstrass model E_D for the $\mathbb{Q}(\sqrt{D})$-quadratic twist having discriminant exactly divisible by either p^3 or by p^9. In either case, this model is minimal at p and has bad reduction at p (*cf.* [52, VII, 1.1, 5.1]. This completes the proof of Lemma 2.1. ∎

We will have recourse to the following.

Corollary 2.2 *If $n \geq 7$ is prime and $abAB$ is divisible by an odd prime p, then the j-invariant $j(E)$ of the curve $E = E_i(a,b,c)$ satisfies*

$$\operatorname{ord}_p\big(j(E)\big) < 0.$$

In particular, if $ab \neq \pm 1$ then $E_i(a,b,c)$ does not have complex multiplication.

Proof By part (b) of Lemma 2.1 the curve $E = E_i(a,b,c)$ has multiplicative reduction at each odd prime p dividing $abAB$. In particular, E does not have potentially good reduction at such a prime p. It then follows that for such a prime p the j-invariant $j(E)$ of E is not a p-adic integer [52, VII, 5.5]. Similarly, if $2|ab$ then, since $n \geq 7$, it follows from Lemma 2.1 that E has multiplicative reduction at 2 and hence $j(E)$ is not a 2-adic integer. In particular, it follows that if $ab \neq \pm 1$, then $j(E)$ is not an integer. From the well-known fact that the j-invariant of an elliptic curve with complex multiplication is an algebraic integer [53, II, Theorem 6.1], we see that if $ab \neq \pm 1$, then E cannot have complex multiplication. ∎

3 Galois Representations

Let $E = E_i(a,b,c)$ for some $1 \leq i \leq 3$ and some primitive solution (a,b,c) to (1.2). We associate to the elliptic curve E a Galois representation

$$\rho_n^E\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n).$$

This is just the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $E[n]$ of the elliptic curve E, having fixed once and for all an identification of $E[n]$ with $\mathbb{F}_n^2$. We continue to make our assumptions that aA, bB and cC are pairwise coprime and that C is squarefree. Without loss of generality we may also suppose that A and B are n-th-power free.

Corollary 3.1 *If $n \geq 7$ is a prime and if $ab \neq \pm 1$, then ρ_n^E is absolutely irreducible.*

Proof Since the representation ρ_n^E is odd, meaning that the image of any complex conjugation has eigenvalues 1 and -1, and since n is odd, ρ_n^E is absolutely irreducible if and only if it is irreducible. Thus we need only rule out the case that ρ_n^E is reducible.

If ρ_n^E is reducible, then E has a $\mathbb{Q}$-rational subgroup of order n. Combining this with part (c) of Lemma 2.1 it follows that E has a $\mathbb{Q}$-rational point of order $2n$. By the work of Mazur [39] and Kubert [33] this cannot happen if $n \geq 17$. It also follows from their work that if $7 \leq n \leq 13$ then the only elliptic curves over $\mathbb{Q}$ having a $\mathbb{Q}$-rational subgroup of order $2n$ also have complex multiplication. Our hypothesis that $ab \neq \pm 1$ together with Corollary 2.2 implies that E does not have complex multiplication and therefore does not have a $\mathbb{Q}$-rational subgroup of order $2n$. It follows that ρ_n^E is irreducible, as claimed. ∎

We can associate to each representation ρ_n^E a number N_n^E called the *conductor* of ρ_n^E. It is defined in [51]; an immediate property of this definition is that N_n^E divides $N(E)$. This can be a strict divisibility, as the following lemma shows.

Lemma 3.2 *If $n \geq 3$ is a prime and ρ_n^E is associated to a primitive solution (a, b, c) of* (1.2)*, then*

$$N_n^E = 2^{\beta} \prod_{p|C, p\neq n} p^2 \prod_{q|AB, q\neq n} q,$$

where

$$\beta = \begin{cases} 1 & \text{if } ab \equiv 0 \pmod 2 \text{ and } AB \equiv 1 \pmod 2 \\ \alpha & \text{otherwise,} \end{cases}$$

for α as defined in the statement of Lemma 2.1.

Proof If $p \neq n$ is a prime at which the curve E has multiplicative reduction (*i.e.*, $p \parallel N(E)$), then a result of Serre (*cf.* [51, (4.1.1.2)]) shows that if also $n | \operatorname{ord}_p\big(\Delta(E)\big)$ then p does *not* divide N_n^E; otherwise $p \parallel N_n^E$. It then follows from this and from parts (a) and (b) of Lemma 2.1 that N_n^E divides $2^{\beta} \prod p^2 \prod q$, where the first product is over primes $p \neq n$ dividing C and the second product is over primes $q \neq n$ dividing AB, and that $\prod q$ divides N_n^E. To prove that N_n^E actually equals the given formula requires an analysis involving the definitions of the p-parts of $N(E)$ and N_n^E for primes $p \neq n$ dividing $2C$.

Let T_n be the n-adic Tate module of the curve E. Fix an isomorphism $T_n \cong \mathbb{Z}_n^2$ and let $\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_n)$ be the Galois representation coming from the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on T_n. Let $p \neq n$ be a prime dividing $2C$ and let D_p and I_p be, respectively, a decomposition group and inertia subgroup at the prime p.

Suppose $p^r \parallel N(E)$ and $p^{r_0} \parallel N_n^E$. A comparison of the definitions of the p-parts of $N(E)$ and N_n^E shows that

$$r - r_0 = \dim_{\mathbb{F}_n}(E[n]^{I_p}) - \operatorname{rank}_{\mathbb{Z}_n}(T_n^{I_p})$$

where the superscript 'I_p' denotes the part fixed under the action of the inertia group I_p. Since $p|N(E)$, the curve E does not have good reduction at p, and hence $\operatorname{rank}_{\mathbb{Z}_n}(T_n^{I_p}) \leq 1$ [52, VII, 7.1].

If $\dim_{\mathbb{F}_n}(E[n]^{I_p}) = 0$ then there is nothing to prove. Suppose then that $\dim_{\mathbb{F}_n}(E[n]^{I_p}) \geq 1$. Since the determinant of ρ_n^E is unramified away from the prime n, the group $\rho_n^E(I_p)$ is contained in a unipotent subgroup of $\mathrm{GL}_2(\mathbb{F}_n)$ and therefore has order dividing n. Since ρ_n^E is equivalent to the reduction of ρ modulo n and since the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}_n) \to \mathrm{GL}_2(\mathbb{F}_n)$ is a pro-n-group, it follows that $\rho(I_p)$ is a pro-n-group. In particular, $\rho|_{I_p}$ factors through the maximal pro-n-quotient of I_p, say $I_p^{(n)}$, which is isomorphic to $\mathbb{Z}_n$.

Let $\tau \in I_p$ be an element mapping to a topological generator of $I_p^{(n)}$. Let $\alpha, \beta \in \overline{\mathbb{Q}}_n^{\times}$ be the eigenvalues of $\rho(\tau)$ and let $\sigma \in D_p$ be any lift of a Frobenius element. From the well-known action of Frobenii on tame inertia we have that $\rho(\sigma\tau\sigma^{-1}) = \rho(\tau^p)$. It follows that $\{\alpha, \beta\} = \{\alpha^p, \beta^p\}$. In particular, α and β must be primitive n^k-th roots of unity, for some nonnegative integer k. Note also that $\beta = \alpha^{-1}$ since $\det\big(\rho(\tau)\big) = 1$, and hence $\alpha + \alpha^{-1} = \operatorname{trace}(\big(\rho(\tau)\big)$ is in $\mathbb{Z}_n$. Since $\mathbb{Q}_n(\alpha + \alpha^{-1})$ has degree $n^{k-1}(n-1)/2$ over $\mathbb{Q}_n$ if $k \geq 1$, it follows that $k = 0$. Therefore $\alpha = \beta = 1$

and $\operatorname{rank}_{\mathbb{Z}_n}(T_n^{I_p}) = 1$. It then follows from the definition of $N(E)$ that $p \parallel N(E)$ (*i.e.*, E has multiplicative reduction at p). From part (b) of Lemma 2.1 it follows that this can occur only if $p = 2$ and we are in case (v) with $\beta = \alpha = 0$ and $\operatorname{ord}_2(Bb^n) \geq 7$. Suppose then that we are in this case.

If $2 \nmid B$ then $2|b$ and $n| \operatorname{ord}_2\big(\Delta(E)\big)$, and so it follows from the aforementioned result of Serre that $2 \nmid N_n^E$, which agrees with the given formula. If $2|B$ then, since $n \nmid \operatorname{ord}_2(B)$ by hypothesis, $n \nmid \operatorname{ord}_2\big(\Delta(E)\big)$ whence, again by Serre's result, $2 \parallel N_n(E)$, which also agrees with the given formula. ∎

We now wish to connect the representations ρ_n^E with representations arising from modular forms. We begin by summarizing what it means for ρ_n^E to be modular.

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

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

unramified at all primes not dividing Mn and such that if $f(z) = \sum_{n=1}^{\infty} c_n q^n$, $q := e^{2\pi i z}$, then

$$\operatorname{trace} \rho_{f,\nu}(\operatorname{Frob}_p) \equiv c_p \pmod{\nu} \tag{3.1}$$

for all p not dividing Mn. Here Frob_p is any Frobenius element at the prime p.

If the representation ρ_n^E, with scalars extended to $\overline{\mathbb{F}}_n$, is equivalent to some $\rho_{f,\nu}$ then we say that ρ_n^E is modular and that it arises from the newform f (or that f gives rise to ρ_n^E).

Lemma 3.3 *Suppose that $n \geq 7$ is a prime and that ρ_n^E is associated to a primitive solution (a, b, c) to (1.2) with $ab \neq \pm 1$. Put*

$$N_n(E) = \begin{cases} N_n^E & n \nmid ABC, \\ nN_n^E & n|AB, \\ n^2 N_n^E & n|C. \end{cases}$$

The representation ρ_n^E arises from a cuspidal newform of weight 2, level $N_n(E)$, and trivial Nebentypus character.

Proof Applying work of Breuil, Conrad, Diamond and Taylor [4] (or even, since, by part (b) of Lemma 2.1, the curve E does not have conductor divisible by 27, earlier work of Conrad, Diamond and Taylor [12]) we may conclude that E is modular. In particular this means that the the representation ρ_n^E is modular. We also know by Corollary 3.1 that ρ_n^E is irreducible. It then follows from work of Ribet [21, Theorem 6.4] that ρ_n^E arises from a cuspidal newform with weight 2, level $N_n(E)$, and trivial Nebentypus character. The key point is that if $n \nmid ABC$ then $n \nmid N_n(E)$ by part (b) of Lemma 2.1, and so $\rho_n^E|_{D_n}$ is 'finite' in the sense of [21]. Similarly, if $n|AB$, then E has multiplicative reduction at n by part (b) of Lemma 2.1, and so $\rho_n^E|_{D_n}$ is 'Selmer' in the sense of [21]. ∎

To make use of this lemma we need to carefully analyse the newforms of level $N_n(E)$ from which our representations can arise. We begin this study in the next section.

4 Eliminating Newforms

We will use a number of different methods to eliminate the possibility of certain newforms of level $N_n(E)$ giving rise to the representation ρ_n^E. These are collected in the main propositions of the following subsections. Variants upon Propositions 4.3 and 4.6 occur, in varying degrees of explicitness, in earlier work of Serre [51] and Kraus [31] (in the first instance) and Darmon and Merel [19] (in the second). Proposition 4.4 appears to be new. As we shall observe in Section 5, many of our Diophantine problems require simultaneous application of Propositions 4.3, 4.4 and 4.6.

4.1 An Absence of Newforms

Proposition 4.1 *Suppose $n \geq 7$ is a prime and that $E = E_i(a, b, c)$ is the curve associated to a primitive solution of* (1.2)*. If*

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

then $ab = \pm 1$.

Proof This is essentially the same argument by which Fermat's Last Theorem was reduced to the modularity of semistable elliptic curves.

If $ab \neq \pm 1$, then, as a consequence of Lemma 3.3, there exists a cuspidal newform of weight 2 and level $N_n(E)$. However, it follows from combining Theorems 2.5.2, 4.2.4, 4.2.7 and 4.2.11 of [42] that there are no non-zero cuspforms of weight 2 and level equal to any of the numbers N listed in the statement of the proposition. From this contradiction it follows that $ab = \pm 1$ whenever $N_n(E)$ is one of the listed numbers. ∎

Of course, this list is quite small and one quickly finds oneself considering $N_n(E)$ for which the corresponding space of cuspforms is non-zero (for example if $A = B = C = 1$ and ab is odd then $N_n(E) = 32$ and there exists a cuspidal newform of weight 2 and level 32). Thus one needs other ways to establish that a given newform of level $N_n(E)$ cannot give rise to ρ_n^E.

4.2 Congruences

By Lemma 2.1, the curves $E_i(a, b, c)$ all have rational 2-torsion. In consequence, we may restrict the possibilities for the Fourier coefficients of the newforms that can give rise to ρ_n^E. Since our curves need not have full rational 2-torsion, we have more difficulty exploiting such arguments than was the case for equations of the shape $x^n + y^n = L^\alpha z^n$, investigated by Serre in [51].

Lemma 4.2 *Suppose $n \geq 7$ is a prime and $E = E_i(a, b, c)$ is a curve associated to a primitive solution of* (1.2). *Suppose also that p is an odd prime not dividing nN_n^E. Then either*

$$\operatorname{trace} \rho_n^E(\operatorname{Frob}_p) = \pm(1 + p)$$

or

$$\operatorname{trace} \rho_n^E(\operatorname{Frob}_p) = \pm 2r,$$

for some integer $r \leq \sqrt{p}$.

Proof Suppose first that $p|ab$. Then E has multiplicative reduction at p. From the well-known theory of Tate-curves [53, V] (see also [52, Appendix C, §15]), it follows that trace $\rho_n^E(\operatorname{Frob}_p) = \pm(1 + p)$.

Suppose then that $p\nmid ab$. In this case the curve E has good reduction at p since $p\nmid N_n(E)$. From the Weil-bounds we know that the number of points N_p on E in the finite field $\mathbb{F}_p$ is given by

$$N_p = p + 1 - a_p$$

for some integer a_p satisfying $-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$. Since p is odd and E has a $\mathbb{Q}$-rational 2-torsion point, 2 divides N_p and hence also a_p. Since

$$\operatorname{trace} \rho_n^E(\operatorname{Frob}_p) \equiv a_p \pmod{n}$$

(*cf.* [53, II, 10.1]) the lemma follows. ∎

As an immediate consequence of this lemma we obtain the following.

Proposition 4.3 *Suppose $n \geq 7$ is a prime and $E = E_i(a, b, c)$ is a curve associated to a primitive solution of* (1.2) *with $ab \neq \pm 1$. Suppose further that*

$$f = \sum_{m=1}^{\infty} c_m q^m \quad (q := e^{2\pi i z})$$

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 one of either*

$$\operatorname{Norm}_{K_f/\mathbb{Q}}\big(c_p \pm (p + 1)\big)$$

or

$$\operatorname{Norm}_{K_f/\mathbb{Q}}(c_p \pm 2r),$$

for some integer $r \leq \sqrt{p}$.

When applying this proposition to a specific newform we often find it necessary to consider c_p for more than one p. The primes p we use vary from form to form. We leave these ad hoc arguments to later sections.

4.3 Images of Inertia

Very often the spaces of cuspforms of level $N_n(E)$ contain newforms associated to elliptic curves with rational 2-torsion. Consequently, the results of neither of the preceding subsections can be used to show that these curves cannot give rise to the representation ρ_n^E. However, as a consequence of part (d) of Lemma 2.1 we have a good understanding of $\rho_n^E(I_p)$ for an inertia group I_p corresponding to an odd prime p dividing C. Often this can be shown to be inconsistent with the properties of the action of inertia on the n-adic Tate-module of the elliptic curves associated to the newforms.

Proposition 4.4 *Suppose $n \geq 3$ is a prime and $E = E_i(a, b, c)$ is a curve associated to a primitive solution of* (1.2). *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.*

Proof Suppose $p \neq n$ is an odd prime dividing C. As in the proof of Lemma 3.2, let $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_n)$ be the Galois representation on the n-adic Tate-module of E. Since, by part (d) of Lemma 2.1, E obtains good reduction over $\mathbb{Q}(\sqrt[4]{C}, \sqrt{-1})$ at all prime ideals dividing p, we have $\#\rho(I_p)|8$ (*cf.* [52, VII, 7.1]). If $\#\rho(I_p) = 2$, then there exists a quadratic field K such that the restriction of ρ to $\mathrm{Gal}(\overline{K}/K)$ is unramified at all prime ideals dividing p, hence E obtains good reduction over K at all such prime ideals, contradicting the second half of part (d) of Lemma 2.1. Thus $4|\#\rho(I_p)$. Since ρ_n^E is equivalent to the reduction of ρ modulo n and since the kernel of this reduction is a pro-n-group, it follows that $4|\#\rho_n^E(I_p)$.

On the other hand, if E' is another elliptic curve defined over $\mathbb{Q}$ such that p divides the denominator of $j(E')$, then E' has potentially multiplicative reduction at p [53, VII, 5.5]. Hence I_p acts on $E'[n]$ via a quotient of $\mathbb{Z}/2 \times \mathbb{Z}_n$ (this follows from the theory of Tate curves [53, V] (but see also [52, Appendix C, §15]). In particular, 4 fails to divide $\#\rho_n^{E'}(I_p)$. It follows that $\rho_n^{E'}$ is not isomorphic to ρ_n^E. ∎

4.4 Hecke Characters and Complex Multiplication

Unfortunately, we will sometimes encounter elliptic curves of conductor $N_n(E)$ having rational 2-torsion and integral j-invariants. These cannot be excluded by the arguments of the preceding subsections. In cases where these curves have complex multiplication they can be treated by variations on the methods of [19]. Before stating our main result of this subsection, we recall some properties of modular forms having complex multiplication.

Let K be an imaginary quadratic field and fix an embedding of K into $\mathbb{C}$ (via which we identify K with a subfield of $\mathbb{C}$). Let $\mathcal{O}_K$ and $\mathbb{A}_K$ be the integer ring and adele ring of K, respectively. By an *algebraic Hecke character* of K we will mean a homomorphism $\chi\colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ that is the identity on $K^\times$ and trivial on $\mathbb{C}^\times$ and on an open subgroup of $\prod_{\mathfrak{p}} \mathcal{O}_{K,\mathfrak{p}}^\times$, where $\mathfrak{p}$ runs over the prime ideals of K. We define the *conductor of* χ

(an integral ideal) by

$$\mathfrak{n}_\chi := \prod_{\mathfrak{p}} \mathfrak{p}^{r_\mathfrak{p}},$$

where

$$r_\mathfrak{p} = \max\{r > 0 : \chi(1 + \mathfrak{p}^{r-1}) \neq 1\}$$

if $\chi(\mathcal{O}_{K,\mathfrak{p}}) \neq 1$ and 0 otherwise. To obtain from χ a Hecke character in the usual sense, we associate to each fractional ideal $\mathfrak{a}$ an adele $a_\mathfrak{a} \in \mathbb{A}_K^\times$ that is trivial at infinity: at a prime ideal $\mathfrak{p}$, $a_{\mathfrak{a},\mathfrak{p}} = \pi^r$ where π is some uniformizer at $\mathfrak{p}$ and $r = \mathrm{ord}_\mathfrak{p}(\mathfrak{a})$. The adele $a_\mathfrak{a}$ is not well-defined, but if (a) is coprime to $\mathfrak{n}_\chi$ then $\chi(a_\mathfrak{a})$ is well-defined. We write $\chi(\mathfrak{a})$ for this value. The character $\mathfrak{a} \mapsto \chi(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{a})^{-\frac{1}{2}}$ is a Hecke character on the group of fractional ideals of modulus $\mathfrak{n}_\chi$. The following lemma is a consequence of [42, Theorem 4.8.2].

Lemma 4.5 *Let K be an imaginary quadratic field. Let d_K be the discriminant of K and let $\chi_K = \left(\frac{d_K}{\cdot}\right)$ be the usual Dirichlet character associated to K. If χ is an algebraic Hecke character of K of conductor $\mathfrak{n}_\chi$, then*

$$f_\chi(z) = \sum_{n=1}^{\infty} \Big(\sum_{\substack{(\mathfrak{a},\mathfrak{n}_\chi)=1 \\ \mathrm{Norm}(\mathfrak{a})=n}} \chi(\mathfrak{a}) \Big) e^{2\pi i n z},$$

where $\mathfrak{a}$ runs over integral ideals of K, is a newform of weight 2 and level $N_\chi = |d_K| \times \mathrm{Norm}\,\mathfrak{n}_\chi$ with Nebentypus character given by $m \mapsto \chi_K(m)\chi((m))|m|^{-1}$.

We will say that a newform f has complex multiplication (or CM) by an imaginary quadratic field K if $f = f_\chi$ for some algebraic Hecke character χ of K.

Proposition 4.6 *Suppose $n \geq 7$ is a prime and $E = E_i(a, b, c)$ is a curve associated to a primitive solution of (1.2) with $ab \neq \pm 1$. Suppose that ρ_n^E arises from a newform having CM by an imaginary quadratic field K. Then one of the following holds:*

(a) *$ab = \pm 2^r$, $r > 0$, $2 \nmid ABC$ and 2 splits in K.*
(b) *$n = 7$ or 13, n splits in K and either $E(K)$ has infinite order for all elliptic curves of conductor $2n$ or $ab = \pm 2^r 3^s$ with $s > 0$ and 3 ramifies in K.*

Before beginning the proof of this proposition, we recall the Galois representations associated to newforms having CM.

Suppose K is an imaginary quadratic field and χ is an algebraic Hecke character of K. Let $L \subseteq \mathbb{C}$ be the subfield generated by the values of χ. This is a finite extension of K. Let n be a prime, ν be a prime of L over n and μ be the prime of K under ν. Define α_ν to be the character $\mathbb{A}_K^\times \to L_\nu^\times$ obtained by composing the natural projection $\mathbb{A}^\times \to K_\mu^\times$ with the inclusion $K_\mu^\times \hookrightarrow L_\nu^\times$. Then α_ν agrees with χ on $K^\times$ and $\chi_\nu = \chi\alpha_\nu^{-1}$ defines a continuous character $\mathbb{A}_K^\times \to L_\nu^\times$ that is trivial on $K^\times$. It then follows from class field theory that χ_ν determines a continuous character $\mathrm{Gal}(\overline{K}/K) \to L_\nu^\times$ that is unramified away from μ and $\mathfrak{n}_\chi$. We will also denote this character by χ_ν.

Since χ_ν is continuous, it actually takes values in $\mathcal{O}_{L,\nu}^\times$, where $\mathcal{O}_{L,\nu}$ is the ring of integers of L_ν. Let $\mathbb{F}_\nu = \mathcal{O}_{L,\nu}/\nu$. Reducing χ_ν modulo ν we obtain a character $\overline{\chi}_\nu\colon \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_\nu^\times$. Let $\rho_{\chi,\nu}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\nu)$ be the induction to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the character $\overline{\chi}_\nu$. It follows easily from the definitions and from the Fourier expansion of f_χ that if $p \nmid 2N_\chi$ then $\rho_{\chi,\nu}$ is unramified at p and that trace $\rho_{\chi,\nu}(\mathrm{Frob}_p)$ is the reduction modulo ν of the p-th Fourier coefficient of f_χ. Thus $\rho_{\chi,\nu}$ is equivalent to the representation $\rho_{f_\chi,\nu}$ (upon extending scalars for the former to $\overline{\mathbb{F}}_\nu$).

Lemma 4.7 *Suppose $n \geq 3$. Let K, χ, and ν be as in the preceding paragraphs.*

(a) $\rho_{f_\chi,\nu}|_{\mathrm{Gal}(\overline{K}/K)}$ *is abelian.*
(b) *If n is inert in K then $\rho_{f_\chi,\nu}\big(\mathrm{Gal}(\overline{K}/K)\big)$ has order divisible by (n^2-1).*
(c) *If n splits in K then $\rho_{f_\chi,\nu}\big(\mathrm{Gal}(\overline{K}/K)\big)$ has order divisible by $(n-1)^2$.*

Proof As mentioned above, $\rho_{f_\chi,\nu}$ is equivalent to $\rho_{\chi,\nu}$, so it suffices to prove the lemma with $\rho_{f_\chi,\nu}$ replaced by $\rho_{\chi,\nu}$.

Let $\overline{\chi}'_\nu$ be the conjugate character of $\overline{\chi}_\nu$ (so if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts non-trivially on K, then $\overline{\chi}'_\nu(\tau) = \chi_\nu(\sigma\tau\sigma^{-1})$ for all $\tau \in \mathrm{Gal}(\overline{K}/K)$). From the definition of $\rho_{\chi,\nu}$ it follows that $\rho_{\chi,\nu}|_{\mathrm{Gal}(\overline{K}/K)}$ is isomorphic to $\overline{\chi}_\nu \oplus \overline{\chi}'_\nu$. This is obviously abelian, so part (a) of the lemma is true.

Let μ be the prime of K above n in the definition of χ_ν. It follows from class field theory that the image under $\overline{\chi}_\nu$ of an inertia group at μ is just $\overline{\chi}_\nu(\mathcal{O}_\mu^\times)$. From the definition of χ_ν it follows that this last group is isomorphic to $(\mathcal{O}_\mu/\mu)^\times$. Part (b) of the lemma follows from this, for if n is inert in K (so $(n) = \mu$) then $|(\mathcal{O}_\mu/\mu)^\times| = (n^2-1)$. Suppose then that n is split in K. Let μ' be the conjugate of the prime μ (so $(n) = \mu\mu'$). Then χ_ν, and hence $\overline{\chi}_\nu$, is unramified at μ', but ramified at μ. Similarly, $\overline{\chi}'_\nu$ is unramified at μ, but ramified at μ', and the image under $\overline{\chi}'_\nu$ of an inertia group at μ' is just $\overline{\chi}_\nu(\mathcal{O}_\mu^\times)$ which is isomorphic to $(\mathcal{O}_\mu/\mu)^\times$. Part (c) follows easily. ∎

We now prove three lemmata that are key to the proof of Proposition 4.6.

Lemma 4.8 *Suppose that n is a prime and that $E = E_i(a,b,c)$ is a curve associated to a primitive solution of* (1.2) *with $ab \neq \pm 1$. Suppose that ρ_n^E arises from a newform having CM by a field K*

(a) *The image of ρ_n^E is the normalizer of a Cartan subgroup.*
(b) *The image of ρ_n^E is the normalizer of a split Cartan subgroup if and only if n splits in K.*
(c) *If $E_{a,c}$ has multiplicative reduction at n, then the image of ρ_n^E is the normalizer of a split Cartan subgroup.*

Recall that a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_n)$ is a maximal abelian subgroup. Such a subgroup has order either (n^2-1) (in which case it is isomorphic to $\mathbb{F}_{n^2}^\times$) or $(n-1)^2$ (in which case it is isomorphic to $\mathbb{F}_n^\times \times \mathbb{F}_n^\times$). In the first case we say that the Cartan subgroup is *non-split* and in the second that it is *split*.

Proof Parts (a) and (b) follow immediately from Lemma 4.7.

Let G be a Cartan subgroup such that the image of ρ_n^E is the normalizer of G. If E has multiplicative reduction at n, then the restriction of ρ_n^E to a decomposition group D_n at n is isomorphic to $\delta\omega \oplus \delta$, where ω is the character giving the action of D_n on the n-th roots of unity and δ is an unramified character of order at most 2. It follows that n splits in K. From part (b) of the lemma it then follows that G is split. This proves part (c). ∎

Lemma 4.9 *Suppose that $n \geq 7$ is a prime and that $E = E_i(a, b, c)$ is associated to a primitive solution of* (1.2) *with $ab \neq \pm 2^r$. If ρ_n^E arises from a newform having CM by a field K, then one of the following holds:*

(a) *The image of ρ_n^E is the normalizer of a non-split Cartan subgroup.*
(b) *$n = 7$ or 13, n splits in K and either $E'(K)$ has infinite order for all elliptic curves E' of conductor $2n$ or $ab = \pm 2^r 3^s$ with $s \geq 0$ and 3 ramifies in K.*

Proof By part (a) of Lemma 4.8 the image of ρ_n^E is the normalizer of a Cartan subgroup. Suppose that this image is not the normalizer of a non-split Cartan subgroup. Then $E[n]$ consists of two K-rational subgroups of order n that are either stable or interchanged by the action of any element in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In particular, the set of these two subgroups is defined over $\mathbb{Q}$. Therefore E defines a $\mathbb{Q}$-rational point on the curve $X_{\mathrm{split}}(n)$ defined in [43]. By [43, Proposition 3.1], if $n \geq 11$, $n \neq 13$, then E has potentially good reduction at all primes $p \neq 2$. This contradicts part (b) of Lemma 2.1 since we have assumed that $ab \neq \pm 2^r$. It remains to deal with the cases $n = 7, 13$.

Suppose then that $n = 7$ or 13. By part (b) of Lemma 4.8 it follows that n splits in K. Also, E together with one of its K-rational subgroups of order n defines a K-rational point x on the modular curve $X_0(2n)$ (recall that E has a $\mathbb{Q}$-rational point of order two). If E' is an elliptic curve of conductor $2n$, then the curve $X_0(2n)$ has as a quotient over $\mathbb{Q}$ the curve E'. If $E'(K)$ has finite order then the image on the curve E' of the point x has finite order. It then follows from [39, Corollary 4.3] that E has potentially good reduction at all primes $p \neq 2$ except possibly at $p = 3$ if 3 ramifies in K. Since we have assumed $ab \neq \pm 2^r$, this contradicts part (b) of Lemma 2.1 unless $ab = \pm 2^r 3^s$ with $s > 0$ and 3 ramifies in K. ∎

Lemma 4.10 *Suppose $n \geq 3$ is a prime and that $E = E_i(a, b, c)$ is a curve associated to a solution of* (1.2). *Suppose also that ρ_n^E arises from a newform having CM by a field K. If the image of ρ_n^E is the normalizer of a non-split Cartan then n does not divide ab.*

Proof If $n|ab$, then by part (b) of Lemma 2.1 the curve E has multiplicative reduction at n. From part (c) of Lemma 4.8 it then follows that the image of ρ_n^E is contained in the normalizer of a split Cartan subgroup. ∎

We are now in a position to prove Proposition 4.6. Suppose first that $ab \neq \pm 2^r$ and that ρ_n^E arises from a newform having CM but that conclusion (b) of the proposition does not hold. Then by Lemma 4.9 the image of ρ_n^E is the normalizer of a non-split

Cartan. Also, by part (c) of Lemma 2.1 the curve E has a $\mathbb{Q}$-rational point of order 2. It then follows from [19, Theorem 8.1] that the j-invariant $j(E)$ of the curve E lies in $\mathbb{Z}[\frac{1}{n}]$. If p is an odd prime dividing ab, then by Corollary 2.2 a positive power of p divides the denominator of $j(E)$. From these two observations it follows that $ab = \pm n^t$ for some $t > 0$ (since we are assuming that $ab \neq \pm 1$), but this contradicts Lemma 4.10.

Suppose next that $ab = \pm 2^r$ with $r > 0$. Suppose also that $2|ABC$ (in which case, $2|B$). From Lemma 3.2 it follows that $2 \parallel N_n(E)$. On the other hand, it is clear from Lemma 4.5 that if χ is an algebraic Hecke character and 2 divides N_χ then so does 4. This contradicts the hypothesis that $N_n(E) = N_\chi$ for some χ. We may therefore suppose that 2 fails to divide ABC. From part (b) of Lemma 2.1 we know that E has multiplicative reduction at 2, and from Lemma 3.2 we know that $2 \nmid N_n(E)$ (*i.e.*, ρ_n^E is unramified at 2). Thus $\mathrm{trace}\big(\rho_n^E(\mathrm{Frob}_2)\big) = \pm 3$ (*cf.* the proof of Lemma 4.2). Since $n \geq 7$, this trace is not zero. This, however, is equivalent to the splitting of 2 in K, since, by hypothesis, ρ_n^E is isomorphic to an induced representation of the form $\rho_{\chi,\nu}$. This completes the proof of Proposition 4.6.

5 Theorems 1.1 and 1.2 for $n \geq 7$ Prime

In general, the major difficulty in applying the results of the previous section lies in actually deriving data for the newforms at a given level, for instance in computing systems of Hecke eigenvalues for a basis of representatives for the Galois conjugacy classes of newforms. Thanks to some remarkable work of William Stein [54], this has recently become realistic, at least provided the desired level is not too large. An invaluable resource in this area is Stein's Modular Forms Database (see the website http://modular.fas.harvard.edu/Tables/).

In what follows we give details of the proof of Theorem 1.1 in the cases $C = 2, 5$ and 17. These examples require application of all the assorted techniques described in the previous section. For other values of C we direct the reader to our Appendix where we provide sufficient data to reconstruct our proofs; further information is available from the authors on request. For our data, we rely extensively on the tables of Stein [54].

5.1 $x^n + y^n = 2z^2$

Suppose that (a, b, c) is a primitive solution of $x^n + y^n = 2z^2$, where $n \geq 7$ is a prime. In this case ab is necessarily odd and we can assume that we are in case (ii). Thus the elliptic curve we consider is just $E = E_1(a, b, c)$ and $N_n(E) = N_n^E = 256$ by Lemma 3.2. It turns out that there are six newforms of weight 2, level 256, and trivial character. Moreover, these newforms all have complex multiplication by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. We give a complete proof of this.

Lemma 5.1 *There are six cuspidal newforms of weight* 2*, level* 256*, and trivial Nebentypus character.*

Proof Let S_r^{new} be the space of weight 2 cuspforms on the usual congruence subgroup $\Gamma_0(2^r)$ spanned by the newforms. Similarly, let S_r^{old} be the space of weight 2 cuspforms on the congruence subgroup $\Gamma_0(2^r)$ spanned by oldforms. Let d_r^{new} and d_r^{old} be the respective dimensions over $\mathbb{C}$ of the spaces S_r^{new} and S_r^{old}. From the theory of newforms we have that

$$d_r^{\text{old}} = \sum_{j=1}^{r-1} (r - j + 1) d_j^{\text{new}}.$$

Combining this with the well-known formula for the dimension of the space of all cuspforms of weight 2 on $\Gamma_0(2^r)$ (see [42, Theorem 4.2.11]) one finds that

$$d_j^{\text{new}} = 0, \quad 1 \leq j \leq 4; \quad d_5^{\text{new}} = d_6^{\text{new}} = 1, \quad d_7^{\text{new}} = 4, \quad d_8^{\text{new}} = 6. \qquad \blacksquare$$

In order to 'write down' these newforms we first describe some algebraic Hecke characters.

Let K be either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. Denote by $\mathcal{O}$ and by $\mathbb{A}_K$ the ring of integers and the adeles of K, respectively. Let w be the unique prime of K above 2 and fix an embedding of K into $\mathbb{C}$. We identify K with a subfield of $\mathbb{C}$ via this embedding. Suppose that $\chi\colon \mathcal{O}_w^\times \to \mathbb{C}^\times$ is a character such that χ is the identity on the units of $\mathcal{O}$ and trivial on $1 + w^r$ for some positive integer r. We extend this to a character of $\mathbb{A}_K^\times$ by setting χ to be trivial on $\mathbb{C}^\times$ and on $\mathcal{O}_v^\times$ if $v \neq w$ and to be the identity on $K^\times$. (Here we have used that $\mathbb{A}_K^\times = K^\times \mathbb{C}^\times \prod_v \mathcal{O}_v^\times$ where v runs over the primes of K.) By abuse of notation we will also denote this character by χ.

Let $r(K) = 6$ if $K = \mathbb{Q}(\sqrt{-1})$ and let $r(K) = 5$ if $K = \mathbb{Q}(\sqrt{-2})$. The tables below give the values on coset representatives of generators of $\mathcal{O}_w^\times/(1 + w^{r(K)})$ of some characters $\chi\colon \mathcal{O}_w^\times \to \mathbb{C}^\times$.

$K = \mathbb{Q}(\sqrt{-1})$

χ	i	$2i-1$	3
χ_1	i	i	-1
χ_2	i	$-i$	-1

$K = \mathbb{Q}(\sqrt{-2})$

χ	-1	3	$1+\sqrt{-2}$
χ_3	-1	1	1
χ_4	-1	1	-1
χ_5	-1	1	i
χ_6	-1	1	$-i$

From these tables one easily sees that the conductor of each χ_i is $w^{r(K)}$. It then follows from these tables and from Lemma 4.5 that each f_{χ_i} is a newform of weight 2, level 256, and trivial character. Moreover, the f_{χ_i} are all distinct, hence it follows from Lemma 5.1 that the set $\{f_{\chi_i} : i = 1, \ldots, 6\}$ is the set of all newforms of weight 2, level 256, and trivial character.

We can now apply the results of Subsection 4.4 to prove that $ab = \pm 1$. Suppose $ab \neq \pm 1$. From Lemma 3.3 it follows that ρ_n^E arises from a newform of weight 2, level 256, and trivial character. We have just observed that such a form has CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. Let K be either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$ and suppose ρ_n^E arises from a newform of level 256 with CM by K. Then, since ab is odd it follows from Proposition 4.6 that $n = 7$ or 13 and that n splits in K. This can only happen if $n = 13$ and $K = \mathbb{Q}(\sqrt{-1})$. Suppose then that this is the case. Since 3 does not ramify in K it follows from Proposition 4.6 that $E'(K)$ has infinite order for all elliptic curves E' of conductor 26. However, both the elliptic curve of conductor 26 denoted 26B in Cremona's tables [13] and its K-quadratic twist, denoted 208D in Cremona's tables, have rank zero. Thus the curve 26B has rank zero over K, a contradiction. This completes the proof of Theorem 1.1 when $C = 2$ and $n \geq 7$ is prime.

5.2 $x^n + y^n = 5z^2$

Suppose now that (a, b, c) is a primitive solution of the equation $x^n + y^n = 5z^2$, for $n \geq 7$ prime. We will write N for $N_n(E)$ where E is the corresponding curve $E_i(a, b, c)$. We will also write c_p for the p-th Fourier coefficient (equivalently, p-th Hecke eigenvalue) of a newform.

We distinguish two cases, according to whether ab is even or odd. In the first instance, it follows from Lemma 3.2 that $N = 50$. There are just two newforms of this level, corresponding to elliptic curves over $\mathbb{Q}$. Each of these forms has $c_3 = \pm 1$, so it follows from Proposition 4.3 that neither can give rise to ρ_n^E. This contradicts Lemma 3.3.

If ab is odd, then Lemma 3.2 implies that $N = 800$. From Stein's tables [54] we find that there are 14 Galois conjugacy classes of forms at this level; we list some Hecke eigenvalues for a number of these:

newform	c_p
$800, 2(B)$	$c_3 = 1$
$800, 5(E)$	$c_3 = 1$
$800, 6(F)$	$c_3 = -1$
$800, 9(I)$	$c_3 = -1$
$800, 10$	$c_3 = \pm\sqrt{5}, c_{19} = \mp 3\sqrt{5}$
$800, 11$	$c_3 = 1 \pm \sqrt{5}$
$800, 12$	$c_3 = \pm 2\sqrt{2}$
$800, 13$	$c_3 = \pm\sqrt{5}, c_{19} = \pm 3\sqrt{5}$
$800, 14$	$c_3 = -1 \pm \sqrt{5}$

Here (and henceforth), we refer to forms via Stein's numbering system (where the additional letter designation is the isogeny class of the corresponding elliptic curves over $\mathbb{Q}$ as tabulated by Cremona [13], provided the form has $\mathbb{Q}$-rational Fourier coefficients).

For the forms in the above table, considering c_3 and applying Proposition 4.3 enables us to eliminate the possibility of our representations arising from all but forms

in the classes 800,10 and 800,13. For such forms $c_3 = \pm\sqrt{5}$ and so, by Proposition 4.3, if ρ_n^E did arise from one of these, then n must divide one of $-5, -1, 11$. Since $n \geq 7$ it must be that $n = 11$. For these forms we also have $c_{19} = \pm 3\sqrt{5}$, whence, again by Proposition 4.3, 11 must divide one of $-45, -41, -29, -9, 36, 355$. Since this fails to occur, none of the forms in the classes 800,10 and 800,13 can give rise to ρ_n^E.

Next, we observe that the forms 800,3(C) and 800,7(G) correspond to isogeny classes of elliptic curves all having j-invariants with denominators divisible by 5 (this can be observed from Cremona's tables [13]). Proposition 4.4 implies that these forms cannot give rise to ρ_n^E.

Finally, the forms 800,1(A), 800,4(D) and 800,8(H) each correspond to isogeny classes of elliptic curves having complex multiplication by $\mathbb{Q}(\sqrt{-1})$ (hence the corresponding newforms have CM by $\mathbb{Q}(\sqrt{-1})$). Invoking Proposition 4.6 and arguing as we did for $C = 2$ shows that these forms also cannot give rise to ρ_n^E.

In conclusion, we have shown that ρ_n^E fails to arise from a newform of weight 2, level $N = 800$ and trivial character. This contradicts Lemma 3.3 and hence ab cannot be odd if $ab \neq \pm 1$. Since ab also cannot be even, it follows that the only primitive solutions (a, b, c) to $x^n + y^n = 5z^2$, $n \geq 7$ a prime, are given by $ab = -1$ and $c = 0$.

5.3 $x^n + y^n = 17z^2$

Let us now suppose that (a, b, c) is a primitive solution to the equation $x^n + y^n = 17z^2$, where $n > 7$ is prime. Again, we write N for $N_n(E)$. If ab is even, it follows that $N = 578$; at this level, there are 9 classes of newforms to consider. The first of these corresponds to an elliptic curve over $\mathbb{Q}$. Since the strong Weil curve in the isogeny class 578,1(A) has j-invariant with denominator $1088 = 2^6 \cdot 17$, we may apply Proposition 4.4 to conclude as desired. The remaining 8 classes of forms of level 578 have Fourier coefficients c_p in fields of the shape $K = \mathbb{Q}(\theta)$ where $f(\theta) = 0$ for f as given in the following table (we also list relevant values of c_p).

newform	$f(\theta)$	c_p
578, 2	$\theta^2 - 2$	$c_5 = \theta, c_{11} = -4\theta$
578, 3	$\theta^2 - 8$	$c_3 = \theta$
578, 4	$\theta^2 - 2$	$c_3 = \theta$
578, 5	$\theta^3 + 3\theta^2 - 6\theta - 17$	$c_3 = \theta, c_{11} = \theta^2 - 7$
578, 6	$\theta^3 - 3\theta^2 - 6\theta + 17$	$c_3 = \theta, c_{11} = -\theta^2 + 7$
578, 7	$\theta^3 - 3\theta^2 + 1$	$c_3 = \theta, c_5 = \theta^2 - 3\theta + 2$
578, 8	$\theta^3 + 3\theta^2 - 1$	$c_3 = \theta, c_5 = -\theta^2 - 3\theta - 2$
578, 9	$\theta^4 - 4\theta^2 + 2$	$c_3 = \theta, c_5 = 2\theta$

For each of these and each prime $p \in \{3, 5, 7, 11\}$, we compute $\mathrm{Norm}_{K/\mathbb{Q}}(c_p \pm 2r)$, where $|r| < \sqrt{p}$ or $|r| = \frac{p+1}{2}$. Considering newform 578,2, we find that

$$|\,\mathrm{Norm}_{K/\mathbb{Q}}(c_5 \pm 2r)| \in \{2, 14, 34\}$$

and

$$|\,\mathrm{Norm}_{K/\mathbb{Q}}(c_{11} \pm 2r)| \in \{4, 16, 28, 32, 112\}.$$

Applying Proposition 4.3 thus leads to a contradiction since $n > 7$ is prime. Similarly,

$$|\operatorname{Norm}_{K/\mathbb{Q}}(c_3 \pm 2r)| \in \{4, 8\}$$

and

$$|\operatorname{Norm}_{K/\mathbb{Q}}(c_3 \pm 2r)| \in \{2, 14\}$$

for newforms 578,3 and 578,4, respectively, while, for newforms 578,5 and 578,6, we have

$$|\operatorname{Norm}_{K/\mathbb{Q}}(c_3 \pm 2r)| \in \{1, 9, 17, 71\}.$$

In this last case, if $|\operatorname{Norm}_{K/\mathbb{Q}}(c_3 \pm 2r)| \in \{17, 71\}$, then, necessarily, $\theta \equiv 0 \pmod{\nu}$ for ν a prime lying above 17, or $\theta \equiv \pm 4 \pmod{\nu}$ for ν a prime lying above 71. Since $c_{11} = \pm(\theta^2 - 7)$, for these forms, it follows that $a_{11} \equiv \pm 7 \pmod{17}$ or $a_{11} \equiv \pm 9 \pmod{71}$. In either case, this contradicts the Weil-bounds.

To this point, we have not had to impose conditions upon the prime n, other than that $n > 7$. For newforms 578,7 and 578,8, we encounter difficulties regarding the exponent $n = 17$. Indeed, if $\theta \equiv 4 \pmod{\nu}$ or $\theta \equiv -4 \pmod{\nu}$, where $\theta^3 - 3\theta^2 + 1 = 0$ or $\theta^3 + 3\theta^2 - 1 = 0$, respectively, and ν is a prime lying above 17, then the Weil-bounds are, in fact, satisfied and we fail to obtain a contradiction through the application of Proposition 4.3. To dispense with the cases $n > 7$, $n \neq 17$, we note that, computing $\operatorname{Norm}_{K/\mathbb{Q}}(c_p \pm 2r)$ for $p = 3$ and $p = 5$ and corresponding values of r, we fail to encounter common prime divisors q with $q \in \{11, 13\}$ or $q \geq 19$. The same is true for newform 578,9. This completes the proof of Theorem 1.1 for $C = 17$, xy even and $n \in \{11, 13\}$ or $n \geq 19$ prime.

If our primitive solution (a, b, c) has ab odd, we are led to consider $N = 9248$. This is the largest level we treat in proving our theorems. The newforms at this level are listed as 9248,1 through 9248,52 in Stein's tables [54]. Forms 9248,1, 9248,2, 9248,3, 9248,4, 9248,8 and 9248,9 all correspond to isogeny classes of elliptic curves over $\mathbb{Q}$ with j-invariants having denominators divisible by 17, enabling the application of Proposition 4.4. Further, the newforms given as 9248,5, 9248,6, 9248,7, 9248,11, 9248,12, 9248,28 and 9248,35 have complex multipication by $\mathbb{Q}(\sqrt{-1})$, while forms 9248,25 and 9248,32 have CM by $\mathbb{Q}(\sqrt{-17})$. Again, it is straightforward to show that the elliptic curve denoted 26B in Cremona's tables has rank 0 over $\mathbb{Q}(\sqrt{-17})$. We note that curve 14A has in fact rank 1 over $\mathbb{Q}(\sqrt{-17})$; this is not problematic, however, as we have assumed that $n > 7$. Since 3 fails to ramify in $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-17})$, we conclude via Proposition 4.6 that none of these forms can give rise to ρ_n^E.

For the remaining Galois conjugacy classes of forms, we appeal to Proposition 4.3. The newforms 9248,10, 9248,13, 9248,14, 9248,15, 9248,16 and 9248,17 have, in each case,

$$|\operatorname{Norm}_{K/\mathbb{Q}}(c_3 \pm 2r)| \in \{2, 4, 6, 8, 10, 14\},$$

contradicting $n > 7$ prime. For newforms 9248,18 through 9248,52, we apply Proposition 4.3 with $p \in \{3, 5, 7\}$, except in the cases of newforms 9248,26 and 9248,29. For example, to treat form 9248,50, we begin by noting that the Fourier coefficients

lie in the field $K = \mathbb{Q}(\theta)$ where

$$\theta^{16} - 200\,\theta^{14} + 15408\,\theta^{12} - 606064\,\theta^{10} + 13415544\,\theta^{8} - 172411616\,\theta^{6} + 1260850112\,\theta^{4} - 4778571328\,\theta^{2} + 7056672016 = 0.$$

Since we have

$$\begin{aligned} &20602538790208607155724 8\,c_3 \\ &\quad = 16482564302003137\,\theta^{15} - 3150534822488198910\,\theta^{13} \\ &\qquad + 225733574609412418090\,\theta^{11} - 7932867313835453957656\,\theta^{9} \\ &\qquad + 147269823725942615164172\,\theta^{7} - 14342844735440940230010 32\,\theta^{5} \\ &\qquad + 66656372088282112952079 92\,\theta^{3} - 10915582211641463120052640\,\theta \end{aligned}$$

and

$$\begin{aligned} &41205077580417214311449 6\,c_5 \\ &\quad = 16482564302003137\,\theta^{15} - 3150534822488198910\,\theta^{13} \\ &\qquad + 225733574609412418090\,\theta^{11} - 7932867313835453957656\,\theta^{9} \\ &\qquad + 147269823725942615164172\,\theta^{7} - 14342844735440940230010 32\,\theta^{5} \\ &\qquad + 66656372088282112952079 92\,\theta^{3} - 11121607599543549191609888\,\theta \end{aligned}$$

we may conclude that

$$\mathrm{Norm}_{K/\mathbb{Q}}(c_3 \pm 2r) \in \{2^4 \cdot 23^2, 2^4 \cdot 47^2, 2^4 \cdot 3023^2\},$$

and

$$\mathrm{Norm}_{K/\mathbb{Q}}(c_5 \pm 2r) \in \{2^{10}, 2^{12}, 2^{12} \cdot 193^2, 2^{10} \cdot 17^2 \cdot 1663^2\}.$$

It therefore follows from Proposition 4.3 that this form cannot give rise to a representation ρ_n^E with $n \geq 7$ prime. The newforms listed as 9248,26 and 9248,29 may be eliminated through similar arguments, only applied to the Fourier coefficients c_3 and c_{29}. We note that we are unable to deal with the equation $x^{11} + y^{11} = 17z^2$ by these techniques since, for example, the newform 9248,30 has coefficients

c_3	c_5	c_7
θ	$-2\theta^3 + 3\theta^2 + 16\theta - 12$	$3\theta^3 - 4\theta^2 - 23\theta + 16$

and

c_{13}	c_{19}	c_{23}
$2\theta^3 - 3\theta^2 - 14\theta + 11$	$2\theta^3 - 4\theta^2 - 15\theta + 14$	$-\theta^3 + 2\theta^2 + 7\theta - 6$

where

$$\theta^4 - 2\theta^3 - 7\theta^2 + 10\theta - 3 = 0.$$

If $\theta \equiv 2 \pmod{\nu}$ for ν a prime lying above 11, it follows that $a_3 \equiv 2 \pmod{11}$, $a_5 \equiv 5 \pmod{11}$, $a_7 \equiv 0 \pmod{11}$, $a_{13} \equiv 9 \pmod{11}$, $a_{19} \equiv 6 \pmod{11}$ and $a_{23} \equiv 8 \pmod{11}$. None of these contradict the Weil-bounds. For $p \geq 29$, we may possibly have $a_p = 0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10$, a complete residue system modulo 11.

To prove the full statements of Theorems 1.1 and 1.2, we are led to consider the following levels N:

$$N \in \{1, 2, 4, 8, 9, 18, 25, 32, 36, 49, 50, 72, 98, 121, 169, 225, 242, 256, 288, 289, 338, 392, 450, 484, 578, 676, 800, 968, 1352, 2304, 3872, 5408, 6400, 7200, 9248\}.$$

We list relevant data for these levels in our Appendix. As noted in our introduction, we are unable to fully extend Theorem 1.1 to the case $C = 7$. In fact, the techniques of the preceding sections may be used to deduce the insolubility of the corresponding equation $x^n + y^n = 7z^2$ in pairwise, coprime, nonzero integers (x, y, z), provided xy is even. If, however, xy is odd, we are led to consider weight 2 newforms of level 1568. Four classes of newforms, namely those denoted 1568,4, 1568,6, 1568,8 and 1568,9 in Stein's tables [54], correspond to elliptic curves over $\mathbb{Q}$ with rational 2-torsion, no CM and $j = -64$. None of our methods suffice to eliminate the possibility of ρ_n^E arising from such a form.

6 Theorems 1.3, 1.4, 1.5, 1.6

The proofs of the theorems referenced here are intrinsically easier than those for Theorems 1.1 and 1.2. Indeed they essentially amount to observing that there are no elliptic curves over $\mathbb{Q}$ with a $\mathbb{Q}$-rational 2-torsion point and conductor N for

$$N \in \{1, 2, 3, 5, 6, 10, 11, 13, 19, 22, 26, 29, 32, 38, 43, 44, 53, 58, 59, 61, 67, 76, 86, 88, 93, 95, 104, 106, 110, 115, 118, 122, 133, 134, 143, 152, 172, 186, 190, 230, 232, 236, 244, 253, 256, 266, 268, 286, 319, 341, 344, 352, 403, 416, 424, 437, 472, 488, 506, 536, 551, 608, 638, 682, 736, 806, 874, 899, 928, 992, 1102, 1280, 1376, 1504, 1696, 1798, 1888, 1952, 2144, 2185, 2272, 2432, 2816, 3328\}.$$

For example, to prove Theorem 1.3 for $AB = 2^\alpha 19^\beta$, with $\alpha\beta \geq 1$, we are led to consider $N = 19$ (for $\alpha = 6$), $N = 38$ (for $\alpha \geq 7$), $N = 76$ (for $\alpha = 2$), $N = 152$ (for $\alpha \in \{2, 4, 5\}$), $N = 608$ (for $\alpha = 3$) and $N = 2432$ (for $\alpha = 1$). For the newforms in the following list, we have one of $c_3 \in \{\pm 1, \pm 3\}$, $c_5 \in \{\pm 1, 3\}$ or

$c_7 = \pm 1$:

newform	newform	newform	newform
19, 1	608, 2	2432, 3	2432, 13
38, 1	608, 3	2432, 4	2432, 15
38, 2	608, 4	2432, 5	2432, 16
76, 1	608, 5	2432, 6	2432, 17
152, 1	608, 6	2432, 7	2432, 18
152, 2	2432, 1	2432, 8	2432, 19
608, 1	2432, 2	2432, 9	2432, 20

In each case, we deduce a contradiction for $n > 7$ from consideration of just a single Fourier coefficient. For the remaining newforms (17 classes), we combine information from c_3, c_5 and c_7 as in the preceding section. In each case, we obtain a contradiction for $n > 11$ prime.

Further details for other values of AB are given in our Appendix; in most situations, it proves sufficient to apply Proposition 4.3 with one of $p = 3, 5, 7$ or 11.

7 The Equation $x^n + y^n = 2z^2$: Small Values of n

To extend the results of the previous sections to all integral values of $n \geq 4$, we may appeal to a variety of arguments, well summarized in Poonen [47]. We will provide details in case $A = B = 1$ and $C = 2$ and note that other equations of the shape (1.2) may be dealt with in a similar fashion.

We begin by noting that if $n = 2$ or 3, this equation has infinitely many solutions in pairwise coprime integers x, y and z. In this second instance, parametrizations for these may be found in work of Rodeja [50] and provide an alternative approach to dealing with the exponents 6 and 9 than the one we pursue here. In case $n = 4$, this is a classical result (see *e.g.* Mordell [44, p. 18]). For $n = 5$, the fact that the only solutions in pairwise coprime integers x, y and z are $(x, y, |z|) = (3, -1, 11), (-1, 3, 11)$ and $(1, 1, 1)$ follows from work of Bruin [5], based on Coleman–Chabauty techniques for determining rational points on curves of genus two.

We are left to treat $n = 6$ and 9. In these cases, the desired result follows from arguments of Poonen [47] treating the analogous equation $x^n + y^n = z^2$. If $n = 6$, we have

$$(x^2 + y^2)(x^4 - x^2y^2 + y^4) = 2z^2$$

and hence

$$x^4 - x^2y^2 + y^4 = \epsilon u^2,$$

where $\epsilon \in \{\pm 1, \pm 3\}$. Since $2z^2$ is positive, we may suppose that $\epsilon \in \{1, 3\}$. In each case, the above equation defines an elliptic curve with rank 0 over $\mathbb{Q}$. It is easy to check that the torsion points over $\mathbb{Q}$ correspond to solutions (x, y, z) to our original equation with $xy = \pm 1$.

If $n = 9$, we may write

$$(x^3 + y^3)(x^6 - x^3y^3 + y^6) = 2z^2$$

and hence have

$$x^6 - x^3y^3 + y^6 = \epsilon u^2,$$

where, again, $\epsilon \in \{1, 3\}$. As observed by Poonen [47], the curve $\epsilon V^2 = U^6 - U^3 + 1$ admits two nonhyperelliptic involutions, with corresponding quotients elliptic curves birational to

$$\epsilon Y^2 = X^3 - 21X + 37$$

and

$$\epsilon Y^2 = X^3 - 9X + 9.$$

If $\epsilon = 1$, the first of these curves has rank 0 over $\mathbb{Q}$ and a torsion group of order 3, corresponding to the known 6 rational points with $U = 0, 1, \infty$ on $V^2 = U^6 - U^3 + 1$. Similarly, if $\epsilon = 3$, the second curve has zero rank over $\mathbb{Q}$ and trivial torsion, corresponding to the two rational points with $U = -1$ on $3V^2 = U^6 - U^3 + 1$. Since we assume that x and y are coprime, it follows that $xy = \pm 1$. This completes the proof of Theorem 1.1 in case $C = 2$.

For other values of C, we argue similarly, appealing to recent work of Bruin [6], who deduced the conclusion of Theorem 1.1 in cases

$$n \in \{4, 5, 6, 9\} \text{ for } C \in \{2, 3, 5, 6, 10, 11, 13, 17\},$$

$$n = 7 \text{ for } C \in \{6, 10, 11, 13, 17\}, \quad n = 11 \text{ for } C \in \{10, 11, 13, 17\},$$

$$n = 13 \text{ for } C = 13 \quad \text{and} \quad n = 17 \text{ for } C = 17.$$

8 Applications to Polynomial-Exponential Equations

Through easy specialization, the results of Theorems 1.1 through 1.6 may be applied to a variety of classical problems on polynomial-exponential Diophantine equations. For small values of the exponents (*i.e.*, those not covered by these theorems), we are typically left to determine the set of integral points on certain curves of genus one or two; extensive literature on such problems exists.

8.1 Powers in Recurrence Sequences

An immediate application of Theorem 1.1 with $C = 2$ yields:

Proposition 8.1 *The Diophantine equation $2x^2 - 1 = y^n$ has only the solutions $(x, y, n) = (1, 1, n)$ and $(x, y, n) = (78, 23, 3)$ in positive integers x, y and n with $n \geq 3$.*

Proof For $n \geq 4$, this follows from Theorem 1.1 with $C = 2$. The equation $2x^2 - 1 = y^3$ yields an elliptic curve, birational to $Y^2 = X^3 + 8$, denoted 576A in Cremona's tables [13], of rank 1. It is easy to show, via, say, lower bounds for linear forms in elliptic logarithms (as implemented, for example, in SIMATH), that the only integral points on this curve are given by

$$(X, Y) = (-2, 0), (1, \pm 3), (2, \pm 4), (46, \pm 312)$$

and hence the only solutions to $2x^2 - 1 = y^3$ are with $(x, y) = (0, -1), (\pm 1, 1)$ and $(\pm 78, 23)$. ■

A consequence of this is that any solution in positive integers x and y to an equation of the shape

$$x^{2n} - dy^2 = 1,$$

with d a positive nonsquare integer and $n > 2$, necessarily satisfies either

$$(x, y, n, d) = (23, 156, 3, 6083)$$

or

$$x^n + y\sqrt{d} = (T_1 + U_1\sqrt{d})^{2k+1}$$

for k a nonnegative integer. Here, T_1 and U_1 are the smallest positive integers for which $T_1^2 - dU_1^2 = 1$. To see this, define sequences of integers T_j and U_j by

$$T_j + U_j\sqrt{d} = (T_1 + U_1\sqrt{d})^j.$$

It is easy to show that $T_{2k} = 2T_k^2 - 1$ and so

$$x^n + y\sqrt{d} = (T_1 + U_1\sqrt{d})^{2k}$$

implies that $x^n = 2T_k^2 - 1$, contradicting the above proposition unless $T_k \in \{1, 78\}$. Since $T_k \geq T_1 > 1$, it follows that $T_k = 78$ and hence $d = 78^2 - 1 = 6083 = 7 \cdot 11 \cdot 79$. Working backwards from the equation $2 \cdot 78^2 - 1 = 23^3$ implies that $(x, y, n, d) = (23, 156, 3, 6083)$, as claimed. We remark that this result strengthens the main theorem of [9].

8.2 The Ramanujan–Nagell Equation and Generalizations

An old question of Ramanujan [48], answered in the affirmative by Nagell [45] is whether all solutions in integers (x, n) of the equation

$$x^2 + 7 = 2^n$$

correspond to $n = 3, 4, 5, 7$ and 15. Subsequently, connections between this result and questions in coding theory and group theory have been noted and various generalizations explored. One such approach involves replacing 7 by any fixed odd integer; in this situation, the definitive result is the following, combining theorems of Beukers [2] and Le [34], [35].

Theorem 8.2 **(Beukers, Le)** *Let D be an odd, positive integer. Then the equation*

$$x^2 + D = 2^n$$

has at most one solution in positive integers x and n, unless $D = 7, 23$ or $2^k - 1$ for some $k \geq 4$. The solutions in these exceptional cases are given by

(1) $D = 7$, $(x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$
(2) $D = 23$, $(x, n) = (3, 5), (45, 11)$
(3) $D = 2^k - 1$ $(k \geq 4)$, $(x, n) = (1, k), (2^{k-1} - 1, 2k - 2)$.

Further, the equation

$$x^2 - D = 2^n$$

has at most three solutions in positive integers x and n, unless $D = 2^{2m} - 3 \cdot 2^{m+1} + 1$ *for* $m \geq 3$ *an integer. In these cases, this equation has four positive solutions, given by*

$$(x, n) = (2^m - 3, 3), (2^m - 1, m + 2), (2^m + 1, m + 3) \quad \textit{and} \quad (3 \cdot 2^m - 1, 2m + 3).$$

In the case where $D > 0$, this has been generalized still further, through use of the primitive divisor theorem of Bilu, Hanrot and Voutier [3], culminating in the recent result of Bugeaud [7] (sharpening earlier work of Le [36]).

Theorem 8.3 **(Bugeaud)** *Let D be an odd, positive integer. Then the equation*

$$x^2 + D^m = 2^n$$

has at most one solution in positive integers x, m and n, unless $D = 7, 23$ *or* $2^k - 1$ *for some* $k \geq 4$. *The solutions in these exceptional cases are given by*

(1) $D = 7$, $(x, m, n) = (1, 1, 3), (3, 1, 4), (5, 1, 5), (11, 1, 7), (181, 1, 15), (13, 3, 9)$
(2) $D = 23$, $(x, n) = (3, 5), (45, 11)$
(3) $D = 2^k - 1$ $(k \geq 4)$, $(x, n) = (1, k), (2^{k-1} - 1, 2k - 2)$.

Applying Theorem 1.2 and a result from [1], the following result, in conjunction with Theorem 8.2, strengthens and generalizes Bugeaud's theorem.

Theorem 8.4 *Let D be an odd, positive integer. Then the equation*

$$x^2 + D^m = 2^n$$

has no solutions in integers (x, m, n) *with* $m > 1$, *unless*

$$(|x|, m, n, D) = (13, 3, 9, 7).$$

The only integer solution (x, m, n) *to the equation*

$$x^2 - D^m = 2^n,$$

with $D > 1$, $m > 2$ *and* $n > 1$, *is given by*

$$(|x|, m, n, D) = (71, 3, 7, 17).$$

Further, if $x^2 \pm D = 2^n$ *has a solution in integers x and n, then*

$$n < 5.55 \log(|D|)$$

unless $(|x|, D, n) = (3, -1, 3)$ *or* $(181, 7, 15)$.

We note that this result was obtained independently by Ivorra [26] (with the exception of the upper bound for n). The restriction to $n > 1$ derives from the unfortunate fact that we are unable to apply the techniques of Theorem 1.2 to resolve the Diophantine equation $x^2 - 2 = y^k$ in integers x, y and k. The exclusion in case $x^2 - D^m = 2^n$ of $D = 1$ is to avoid the (almost) trivial case that $3^2 - 1^m = 2^3$. We observe that the equation $|x^2 - y^n| = 1$ in integers $x, y, n > 1$ has been completely solved by Chao Ko [28].

Proof Applying Theorem 1.2, we find that the equation

$$x^m + 2^n y^m = z^2$$

has no solution in odd, paiwise coprime integers x, y and z, with $xy \neq \pm 1$, provided $m \geq 7$ is prime and $n \geq 2$. It follows, if $D > 2$ is odd, that

$$x^2 \pm D^m = 2^n$$

is insoluble for all $m \geq 7$ prime (provided $n \geq 2$). Since $xD \equiv 1 \pmod 2$ and $n \geq 2$, if m is even,

$$x^2 + D^m \equiv 2 \pmod 4,$$

a contradiction. If $x^2 - D^2 = 2^n$ has a solution, then, factoring the left hand side, it follows that $D = 2^k - 1$ and $|x| = 2^k + 1$ for some positive integer k. Since an old result of Lebesgue assures us that $2^k - 1$ is never a perfect power, provided only that $k \geq 2$, it follows that $x^2 - D^m = 2^n$ is insoluble for $D > 1$ and $m > 2$ even.

It remains to deal with $x^2 \pm D^m = 2^n$ with $m \in \{3, 5\}$. In the first case, we may apply work of Coghlan [10] to conclude that the only solution to $x^2 - D^3 = 2^n$ with $D > 1$ odd and $n > 1$ is given by $(|x|, D, n) = (71, 17, 7)$, while the sole solution to $x^2 + D^3 = 2^n$ with $n, D > 1$, D odd, corresponds to $(|x|, D, n) = (13, 7, 9)$. If, on the other hand, $m = 5$, applying work of Bruin [5], we find that the equation $x^2 \pm D^5 = 2^n$ has no solutions whatsoever with $n, D > 1$ and D odd. This result depends upon explicit determination of the rational points on certain curves of genus 2, via an elaboration of the method of Coleman and Chabauty; the reader is directed to [5] for an excellent overview of this subject.

Finally, we note that the upper bound upon n is an immediate consequence of Corollary 1.7 of [1]. This completes the proof of Theorem 8.4. ■

Examination of the above proof reveals that one may obtain similar results, through application of Theorem 1.3, with 2^n replaced by k^n for, by way of example, $k \in \{11, 13, 19, 29, 43, 53, 59, 61, 67\}$.

A second generalization of the Ramanujan–Nagell equation involves equations of the form

$$x^2 + D = y^n \tag{8.1}$$

for fixed integer $D \neq 0$. A fine summary of the extensive body of work on such equations can be found in Cohn [11]. While these equations are, for each $D \neq 0$,

effectively solvable via lower bounds for linear forms in (complex or p-adic) logarithms of algebraic numbers, it can be an extremely involved computational problem to apply such methods to explicitly find all the solutions to an equation of type (8.1). Techniques to fully solve (8.1), for instance in case $D = 1, 2, 3, 4, 5, 6$, have traditionally instead relied upon factorizations in $\mathbb{Q}(\sqrt{-D})$ and straightforward algebraic arguments; recently, the primitive divisor theorem of Bilu, Hanrot and Voutier [3] has played a prominent role (see *e.g.* [7] and [8]). If $D < 0$ or if $D > 0$ and $D \equiv 7 \pmod 8$, however, these methods will in general fail to solve (8.1), due to the presence of infinite units in the quadratic field in question, or to the splitting of the prime 2, respectively. Results based upon the techniques of this paper do not, for the most part, encounter these difficulties. In particular, in case $D > 0$ and $D \equiv 7 \pmod 8$, we may prove the following:

Proposition 8.5 *If $n \geq 3$ is an integer and $D \in \{55, 95\}$, then the only positive integral solutions x, y of the Diophantine equation*

$$x^2 + D = y^n$$

are given by $(x, y, n, D) = (3, 2, 6, 55)$, $(3, 4, 3, 55)$, $(419, 56, 3, 55)$, $(11, 6, 3, 95)$, $(529, 6, 7, 95)$.

Proof We first note that, from work of Ljunggren [38], we may assume, in each case under consideration, that y is even. A solution to $x^2 + D = y^n$ with n odd thus corresponds to a solution in coprime integers $(y, -1, x)$ to $a^n + Db^n = c^2$ with $ab = -y$ even. By Theorem 1.5, we may therefore suppose, without loss of generality, that $n \in \{3, 4, 5, 11\}$ if $D = 55$ and $n \in \{3, 4, 5, 7, 19\}$ if $D = 95$. For $n = 4$, we may solve (8.1) by writing D as a difference of squares. If, however, $n \in \{3, 5, 7, 11, 19\}$, we may reduce equation (8.1) to a system of n-th degree Thue equations and solve them using lower bounds for linear forms in logarithms of algebraic numbers, in conjunction with lattice basis reduction techniques. Nowadays, for equations of small degree (say < 30 or so), it is a relatively routine matter (at least generically) to solve such equations (see *e.g.* Lesage [37] and Mignotte and de Weger [41] for explicit applications of these techniques to equation (8.1)). We suppress the details. ∎

With some work, we can extend this result to treat equation (8.1) for the following squarefree values of $D \equiv 7 \pmod 8$, $D \leq 400$:

$$D = 143, 159, 167, 191, 215, 239, 263, 311, 319, 327, 335, 359, 383, 397.$$

We note that, following arguments of Ivorra [27], it should be possible to characterize those primes $D \equiv 7 \pmod 8$ for which the methods of this paper lead to solution of (8.1).

9 Acknowledgements

The authors would like to thank William Stein for his kind help in performing many of the computations cited herein. They also express gratitude to Nils Bruin, Wilfrid Ivorra and Alain Kraus for helpful discussions and for sharing their recent results.

10 Appendix

In what follows, we will tabulate certain data which should enable the reader to reconstruct our proofs of particular instances of Theorem 1.1, 1.2, 1.3, 1.4, 1.5 and 1.6. As mentioned previously, this is derived principally from Stein's modular forms database.

We begin by listing those newforms to which Propositions 4.4 and 4.6 can be profitably applied. For the first two of our theorems, we may utilize Proposition 4.6 to deal with those newforms encountered with complex multiplication by an imaginary quadratic field. We list these forms (and the corresponding fields) in Table 1.

newform	CM field	newform	CM field	newform	CM field
$32,1$	$\mathbb{Q}(\sqrt{-1})$	$2304,16$	$\mathbb{Q}(\sqrt{-1})$	$6400,7$	$\mathbb{Q}(\sqrt{-1})$
$36,1$	$\mathbb{Q}(\sqrt{-3})$	$2304,17$	$\mathbb{Q}(\sqrt{-3})$	$6400,8$	$\mathbb{Q}(\sqrt{-1})$
$49,1$	$\mathbb{Q}(\sqrt{-7})$	$2304,18$	$\mathbb{Q}(\sqrt{-6})$	$6400,13$	$\mathbb{Q}(\sqrt{-1})$
$121,1$	$\mathbb{Q}(\sqrt{-11})$	$2304,22$	$\mathbb{Q}(\sqrt{-3})$	$6400,18$	$\mathbb{Q}(\sqrt{-2})$
$225,1$	$\mathbb{Q}(\sqrt{-3})$	$2304,23$	$\mathbb{Q}(\sqrt{-6})$	$6400,19$	$\mathbb{Q}(\sqrt{-1})$
$225,2$	$\mathbb{Q}(\sqrt{-3})$	$2304,24$	$\mathbb{Q}(\sqrt{-2})$	$6400,20$	$\mathbb{Q}(\sqrt{-1})$
$225,6$	$\mathbb{Q}(\sqrt{-15})$	$2304,26$	$\mathbb{Q}(\sqrt{-6})$	$6400,32$	$\mathbb{Q}(\sqrt{-2})$
$256,1$	$\mathbb{Q}(\sqrt{-1})$	$3872,1$	$\mathbb{Q}(\sqrt{-1})$	$6400,40$	$\mathbb{Q}(\sqrt{-10})$
$256,2$	$\mathbb{Q}(\sqrt{-2})$	$3872,2$	$\mathbb{Q}(\sqrt{-1})$	$6400,42$	$\mathbb{Q}(\sqrt{-2})$
$256,3$	$\mathbb{Q}(\sqrt{-1})$	$3872,8$	$\mathbb{Q}(\sqrt{-1})$	$6400,44$	$\mathbb{Q}(\sqrt{-2})$
$256,4$	$\mathbb{Q}(\sqrt{-2})$	$3872,15$	$\mathbb{Q}(\sqrt{-1})$	$6400,52$	$\mathbb{Q}(\sqrt{-2})$
$288,1$	$\mathbb{Q}(\sqrt{-1})$	$3872,17$	$\mathbb{Q}(\sqrt{-1})$	$6400,60$	$\mathbb{Q}(\sqrt{-10})$
$288,2$	$\mathbb{Q}(\sqrt{-1})$	$3872,20$	$\mathbb{Q}(\sqrt{-1})$	$6400,63$	$\mathbb{Q}(\sqrt{-2})$
$288,4$	$\mathbb{Q}(\sqrt{-1})$	$3872,22$	$\mathbb{Q}(\sqrt{-1})$	$6400,65$	$\mathbb{Q}(\sqrt{-10})$
$484,2$	$\mathbb{Q}(\sqrt{-11})$	$3872,26$	$\mathbb{Q}(\sqrt{-1})$	$6400,70$	$\mathbb{Q}(\sqrt{-2})$
$800,1$	$\mathbb{Q}(\sqrt{-1})$	$5408,1$	$\mathbb{Q}(\sqrt{-1})$	$6400,71$	$\mathbb{Q}(\sqrt{-5})$
$800,4$	$\mathbb{Q}(\sqrt{-1})$	$5408,5$	$\mathbb{Q}(\sqrt{-1})$	$6400,73$	$\mathbb{Q}(\sqrt{-2})$
$800,8$	$\mathbb{Q}(\sqrt{-1})$	$5408,11$	$\mathbb{Q}(\sqrt{-1})$	$9248,5$	$\mathbb{Q}(\sqrt{-1})$
$800,11$	$\mathbb{Q}(\sqrt{-5})$	$5408,15$	$\mathbb{Q}(\sqrt{-1})$	$9248,6$	$\mathbb{Q}(\sqrt{-1})$
$800,14$	$\mathbb{Q}(\sqrt{-5})$	$5408,20$	$\mathbb{Q}(\sqrt{-13})$	$9248,7$	$\mathbb{Q}(\sqrt{-1})$
$2304,1$	$\mathbb{Q}(\sqrt{-1})$	$5408,23$	$\mathbb{Q}(\sqrt{-1})$	$9248,11$	$\mathbb{Q}(\sqrt{-1})$
$2304,2$	$\mathbb{Q}(\sqrt{-1})$	$5408,25$	$\mathbb{Q}(\sqrt{-1})$	$9248,12$	$\mathbb{Q}(\sqrt{-1})$
$2304,3$	$\mathbb{Q}(\sqrt{-2})$	$5408,29$	$\mathbb{Q}(\sqrt{-13})$	$9248,25$	$\mathbb{Q}(\sqrt{-17})$
$2304,8$	$\mathbb{Q}(\sqrt{-1})$	$5408,32$	$\mathbb{Q}(\sqrt{-1})$	$9248,28$	$\mathbb{Q}(\sqrt{-1})$
$2304,9$	$\mathbb{Q}(\sqrt{-1})$	$6400,1$	$\mathbb{Q}(\sqrt{-1})$	$9248,32$	$\mathbb{Q}(\sqrt{-17})$
$2304,10$	$\mathbb{Q}(\sqrt{-1})$	$6400,6$	$\mathbb{Q}(\sqrt{-1})$	$9248,35$	$\mathbb{Q}(\sqrt{-1})$
$2304,11$	$\mathbb{Q}(\sqrt{-2})$				

Table 1

Let us note that the elliptic curve denoted 14A in Cremona's tables has rank 0 over

$\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$, and rank 1 over the fields $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-13})$ and $\mathbb{Q}(\sqrt{-17})$. It follows, for the forms listed above, that we encounter difficulties with exponent $n = 7$ only for the newforms with CM by one of these 5 fields (*e.g.* forms 800,11, 800,14, *etc.*). As noted in Subsection 5.2, we may in fact employ Proposition 4.3 to treat the case $n = 7$ for forms 800,11 and 800,14 (and, indeed, in several of the the other remaining cases). Similarly, curve 26A has rank 0 over $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-13})$, and positive rank over $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-10})$ and $\mathbb{Q}(\sqrt{-17})$. For each of these last five mentioned fields, curve 26B has rank zero. We may thus eliminate the possibility of solutions corresponding to $n = 13$ for all of the above forms.

We are able to apply Proposition 4.4 precisely when we encounter modular forms, of level a multiple of C^2, corresponding to elliptic curves over $\mathbb{Q}$ with j-invariants having denominators divisible by odd primes dividing C. For the values of C occuring in Theorems 1.1 and 1.2, these are just the following forms:

newform	newform	newform	newform
72, 1	450, 1	800, 7	2304, 15
98, 1	450, 3	2304, 4	9248, 1
225, 3	450, 4	2304, 5	9248, 2
288, 3	450, 5	2304, 6	9248, 3
288, 5	450, 6	2304, 7	9248, 4
289, 1	578, 1	2304, 12	9248, 8
392, 3	676, 1	2304, 13	9248, 9
392, 5	800, 3	2304, 14	

For the remaining forms corresponding to equations covered by Theorems 1.1 through 1.6 (the vast majority), we apply Proposition 4.3. In most instances, we are able to conclude as desired through consideration of only the Fourier coefficients c_3, c_5, c_7 and c_{11}. For certain newforms, however, we need to compute somewhat futher. Below, we list all the forms for which this is the case:

newform	coefficients	newform	coefficients	newform	coefficients
67, 1	c_{17}	800, 10	c_3, c_{19}	2185, 7	c_3, c_7, c_{13}
133, 1	c_3, c_{13}	800, 13	c_3, c_{19}	3328, 35	c_3, c_7, c_{19}, c_{23}
169, 1	c_5, c_{17}, c_{19}	806, 9	c_3, c_{23}	3328, 37	c_3, c_7, c_{19}, c_{23}
169, 2	c_3, c_{23}	899, 5	c_3, c_{19}	3328, 39	c_3, c_7, c_{19}, c_{23}
225, 4	c_7, c_{13}	1102, 7	c_7, c_{31}	3328, 40	c_3, c_7, c_{19}, c_{23}
225, 5	c_7, c_{13}	1280, 2	c_3, c_{13}	3872, 35	c_3, c_5, c_{17}
268, 1	c_{17}	1280, 8	c_3, c_{13}	3872, 37	c_3, c_5, c_{17}
344, 1	c_{13}	1280, 13	c_3, c_{13}	9248, 26	c_3, c_{29}
344, 3	c_3, c_{19}	1280, 16	c_3, c_{13}	9248, 29	c_3, c_{29}
424, 1	c_3, c_{13}	1696, 15	c_3, c_{19}		
488, 3	c_3, c_{19}	2144, 1	c_{17}		
638, 1	c_3, c_{13}	2144, 2	c_{17}		
638, 2	c_3, c_{13}	2185, 1	c_{11}, c_{19}		
682, 3	c_3, c_{23}	2185, 2	c_7, c_{17}		

Further data is available from the authors on request, including complete lists of the Fourier coefficients employed in the application of Proposition 4.3.

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] F. Beukers, *On the generalized Ramanujan–Nagell equation I.* Acta Arith. **38**(1980/1), 389–410.

[3] Y. Bilu, G. Hanrot and P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers.* J. Reine Angew. Math. **539**(2001), 75–122.

[4] 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.

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

[6] ———, *Some low degree ternary equations of signature* $(p, p, 2)$. Preprint.

[7] Y. Bugeaud, *On some exponential Diophantine equations.* Monatsh. Math. **132**(2001), 193–197.

[8] Y. Bugeaud and T. Shorey, *On the number of solutions of the generalized Ramanujan–Nagell equation.* J. Reine Angew. Math. **539**(2001), 55–74.

[9] Z. Cao, *On the Diophantine equation* $x^{2n} - Dy^2 = 1$. Proc. Amer. Math. Soc. (1) **98**(1986), 11–16.

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

[11] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$. Acta Arith. **65**(1993), 367–381

[12] B. Conrad, F. Diamond and R. Taylor, *Modularity of certain potentially Barsotti–Tate Galois representations.* J. Amer. Math. Soc. **12**(1999), 521–567.

[13] J. Cremona, *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992.

[14] H. Darmon, *On the equations* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$. Internat. Math. Res. Notices **72**(1993), 263–274.

[15] ———, *The equation* $x^4 - y^4 = z^p$. C. R. Math. Rep. Acad. Sci. Canada **15**(1993), 286–290.

[16] ———, *Modularity of fibres in rigid local systems.* Ann. of Math. **149**(1999), 1079–1086.

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

[18] 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.

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

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

[21] ———, *The refined conjecture of Serre.* In: Elliptic Curves, Modular Forms, and Fermat's Last Theorem (ed. J. Coates), International Press, Cambridge, MA, 1995, 22–37.

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

[23] G. Frey, *Links between stable elliptic curves and certain Diophantine equations.* Ann. Univ. Sarav. Ser. Math. (1) **1**, 1986.

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

[25] Y. Hellegouarch, *Sur l'équation diophantienne* $x_1^{p^h} + x_2^{p^h} = cx_3^{p^h}$. C. R. Acad. Sci. Paris Sér. A–B **274**(1972), A1385–A1387.

[26] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^p = z^2$ *et* $x^p + 2^\beta y^p = 2z^2$. Preprint.

[27] ———, Personal communication.

[28] Chao Ko, *On the Diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$. Sci. Sinica **14**(1965), 457–460.

[29] 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. (9) **322**(1996), 809–812.

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

[31] ———, *Majorations effectives pour l'équation de Fermat généralisée.* Canad. J. Math (6) **49**(1997), 1139–1161.

[32] ———, *On the equation* $x^p + y^q = z^r$*: a survey.* Ramanujan J. (3) **3**(1999), 315–333.

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

[34] Maohua Le, *On the number of solutions of the generalized Ramanujan–Nagell equation* $x^2 - D = 2^{n+2}$. Acta Arith. **60**(1991), 149–167.

[35] ———, *On the generalized Ramanujan–Nagell equation* $x^2 - D = 2^{n+2}$. Trans. Amer. Math. Soc. **334**(1992), 809–825.
[36] ———, *The Diophantine equation* $x^2 + D^m = 2^{n+2}$. Comment. Math. Univ. St. Paul. **43**(1994), 127–133.
[37] J.-L. Lesage, *Différence entre puissances et carrés d'entiers.* J. Number Theory (2) **73**(1998), 390–425.
[38] W. Ljunggren, *On the Diophantine equation* $Cx^2 + D = y^n$. Pacific J. Math. **14**(1964), 585–596.
[39] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. **44**(1978), 129–162.
[40] L. Merel, *Arithmetic of elliptic curves and Diophantine equations.* J. Théor. Nombres Bordeaux **11**(1999), 173–200.
[41] M. Mignotte and B. M. M. de Weger, *On the Diophantine equations* $x^2 + 74 = y^5$ *and* $x^2 + 86 = y^5$. Glasgow Math. J. (1) **38**(1996), 77–85.
[42] T. Miyake, *Modular Forms.* Springer-Verlag, Berlin-New York, 1988.
[43] F. Momose, *Rational points on the modular curves* $X_{\mathrm{Split}}(p)$. Compositio Math. **52**(1984), 115–137.
[44] L. J. Mordell, *Diophantine Equations.* Academic Press, London, 1969.
[45] T. Nagell, *The diophantine equation* $x^2 + 7 = 2^n$. Ark. Math. **4**(1960), 185–187.
[46] I. Papadopolous, *Sur la classification de Neron des courbes elliptiques en caracteristique residuelle 2 et 3.* J. Number Theory **44**(1993), 119–152.
[47] B. Poonen, *Some Diophantine equations of the form* $x^n + y^n = z^m$. Acta Arith. **86**(1998), 193–205.
[48] S. Ramanujan, *Question 464.* J. Indian Math. Soc. **5**(1913), 120.
[49] K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$. Acta Arith. **79**(1997), 7–16.
[50] F. E. G. Rodeja, *On the diophantine equation* $x^3 + y^3 = 2z^2$. (Spanish) Revista Mat. Hisp.-Amer. (4) **13**(1953), 229–240.
[51] 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.
[52] J. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Math. **106**, Springer-Verlag, Berlin-New York, 1986.
[53] ———, *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Math. **151**, Springer-Verlag, Berlin-New York, 1994.
[54] W. Stein, *Modular forms database.* Current web address http://modular.fas.harvard.edu/Tables/
[55] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141**(1995), 443–551.

Department of Mathematics
University of British Columbia
Vancouver, BC
V6T 1Z2

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA