Ann. Sci. Math. Québec **35**, No 1, (2011), 1–15

TWISTED EXTENSIONS OF THE CUBIC CASE OF FERMAT'S LAST THEOREM

MICHAEL A. BENNETT, FLORIAN LUCA AND JAMIE MULHOLLAND

For Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Nous classifions les premiers p pour lesquels il existe des courbes elliptiques $E/\mathbb{Q}$ de conducteur $N_E \in \{18p, 36p, 72p\}$ avec une 2-torsion rationnelle non triviale. En conséquence, nous montrons que, pour « presque tout » premier p, l'équation diophantienne

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

où $n \geq 4$ et α est un entier positif, possède au plus un nombre fini de solutions en entiers non nuls copremiers x, y et z. Pour prouver ce résultat, nous faisons appel à des techniques disparates telles que les bornes inférieures des formes linéaires en logarithmes p-adiques, le théorème du sous-espace de Schmidt, et des méthodes basées sur les courbes de Frey et sur la modularité des représentations galoisiennes associées.

ABSTRACT. We classify primes p for which there exist elliptic curves $E/\mathbb{Q}$ with conductor $N_E \in \{18p, 36p, 72p\}$ and nontrivial rational 2-torsion. In consequence, we show that, for "almost all" primes p, the Diophantine equation

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

has at most finitely many solutions in coprime nonzero integers x, y and z and positive integers α and $n \geq 4$. To prove this result, we appeal to such disparate techniques as lower bounds for linear forms in p-adic logarithms, Schmidt's Subspace Theorem, and methods based upon Frey curves and modularity of associated Galois representations.

1. Introduction

There are many aspects to what we might deem the "typical" arithmetic behaviour of elliptic curves $E/\mathbb{Q}$ which are understood less well than we would like. The study of, for example, the average Mordell-Weil rank of such curves is intimately connected, via the conjecture of Birch and Swinnerton-Dyer, to the vanishing of associated L-functions. In this regard, it is still unknown whether a positive proportion of elliptic curves $E/\mathbb{Q}$ (by some measure) have positive rank (but see the remarkable recent work of Bhargava and Shankar [1], [2]; an excellent overall survey in this area is [3].) There are a number of senses in which one might claim that a typical elliptic curve $E/\mathbb{Q}$ has only trivial rational torsion. It is possible to make such a statement precise for elliptic

Reçu le 20 août 2009 et, sous forme définitive, le 12 janvier 2010.

curves with prescribed bad reduction at only a few primes. In particular, one may prove the following result (see [4]).

Theorem 1.1. *For a set of primes p of density one, every elliptic curve $E/\mathbb{Q}$ with good reduction outside the set $\{2, 3, p\}$ and multiplicative reduction at p has trivial rational torsion.*

By this, we mean that the set P of primes for which there exists an $E/\mathbb{Q}$ with conductor $N_E = 2^\alpha 3^\beta p$ and $\#E(\mathbb{Q})_{tors} > 1$ has the property that

$$\#\{p \leq X \ : \ p \in P\} = o\left(\pi(X)\right) \ \text{ as } \ X \to \infty.$$

It is worth noting (see *e.g.* [16]) that Theorem 1.1 cannot be extended to the case of additive reduction at p, as there exist elliptic curves $E/\mathbb{Q}$ of conductor kp^2 with a rational 2-torsion point, for every prime $p > 3$, and each

$$k \in \{32, 64, 256, 288, 576, 2304\}.$$

A result such as Theorem 1.1 has immediate consequences for Diophantine equations. Indeed, a common obstruction to applying techniques based upon Frey curves and modular Galois representations to Diophantine problems is the presence of elliptic curves over $\mathbb{Q}$ at appropriate levels with rational isogenies corresponding to those possessed by the Frey curves. For instance, if one wishes (as in, say, Kraus [12]) to show that the equation

$$x^3 + y^3 = z^n \tag{1}$$

has no solutions in coprime nonzero integers x, y and z, for $n \geq 3$, then the presence of an elliptic curve $E/\mathbb{Q}$ at level 72 with full rational 2-torsion represents a serious barrier to progress (but see the remarkable recent paper of Chen and Siksek [7], who prove that (1) has no such solutions for infinitely many n, including those $n \equiv 2$ or $3 \pmod 5$ with $n \geq 5$).

Though equation (1) is currently still somewhat intractable, in this paper we will study "twisted" versions of this equation with the property that the corresponding Diophantine equation may be shown to have at most finitely many solutions. In particular, if S is the set of primes $p \geq 5$ for which there exists an elliptic curve $E/\mathbb{Q}$ with conductor $N_E \in \{18p, 36p, 72p\}$ and at least one nontrivial rational 2-torsion point, then we will prove the following.

Theorem 1.2. *Suppose that $p \geq 5$ is prime and that $p \notin S$. Let $\alpha \geq 1$ be an integer. Then the equation*

$$x^3 + y^3 = p^\alpha z^n \tag{2}$$

has no solutions in coprime nonzero integers x, y and z, and prime n satisfying $n \geq p^{2p}$.

To complement this, we will deduce a less general version of Theorem 1.1, with more precise upper bounds for the counting function of S.

Theorem 1.3. *Let $\pi_S(x) = \#\{p \leq x \ : \ p \in S\}$. Then*

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

Here and henceforth, the implied constant in the Vinogradov symbol is absolute. In truth, it is not even known that S is an infinite set (though we expect that $\log \pi_S(x) \sim \frac{1}{2}\log x$). The fact that "most" primes p have the property that $E/\mathbb{Q}$ with conductors $18p, 36p$ and $72p$ have no nontrivial rational 2-torsion, however, is not obvious from a cursory examination of available data. Indeed, the set S contains every prime p with $5 \leq p \leq 193$. One can check from Cremona's tables, however, that in the interval $[1, 1000]$, the primes

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

lie outside S. In fact, it is rather easy to show that a positive proportion of all primes are in the complement of S, most readily by noting (as we will show later) that S contains no primes p satisfying $p \equiv 317$ or $1757 \pmod{2040}$.

As an immediate consequence of Theorems 1.2 and 1.3, together with a result of Darmon and Granville [8] (which implies, for fixed values of $n \geq 4$ and p, that the equation $x^3 + y^3 = p^\alpha z^n$ has at most finitely many solutions in coprime nonzero integers x, y and z), we have the following.

Corollary 1.4. *There exists a set T of natural density one in the primes such that for every prime $p \in T$, equation (2) has at most finitely many solutions in coprime nonzero integers x, y and z, and integers $\alpha \geq 1$, $n \geq 4$. In particular, this is true for all primes $p \notin S$.*

It is interesting (and nontrivial) to note that there is a bijection between isogeny classes of elliptic curves $E/\mathbb{Q}$ with rational 2-torsion and conductor $144p$, and those with rational 2-torsion and conductor in the set $\{9p, 18p, 36p, 72p\}$, via twists. With this in mind, we could replace Theorem 1.2 with a marginally weaker if cleaner statement, substituting for S the set S' of primes p for which there exists an elliptic curve $E/\mathbb{Q}$ with conductor $144p$ and a rational 2-torsion point.

2. Frey curves and Galois representations

Here and henceforth, we let $p \geq 5$ be prime, $p \notin S$ (so that $p = 197$ or $p \geq 317$), and α be a positive integer. Further, suppose that n is prime with $n \geq p^{2p}$; for most of our arguments, we will in fact only require $n \geq 7$, but even a slightly stronger assumption simplifies matters a bit. We will assume that we have a proper, nontrivial solution (a, b, c) of the equation

$$a^3 + b^3 = p^\alpha c^n,$$

i.e., a solution with a, b and c coprime nonzero integers. We suppose further, without loss of generality, that the following conditions are satisfied :

$$ac \text{ is even, and } b \equiv \begin{cases} -1 \pmod 4 & \text{if } c \text{ is even,} \\ 1 \pmod 4 & \text{if } c \text{ is odd.} \end{cases} \tag{3}$$

Darmon and Granville [8] associate to the triple (a, b, c) the elliptic curve

$$E_{a,b} \ : \ y^2 = x^3 + 3abx + b^3 - a^3, \tag{4}$$

which has a point of order two given by $(x, y) = (a - b, 0)$. The standard invariants $c_4(a, b), c_6(a, b)$ and $\Delta(a, b)$ attached to $E_{a,b}$ are

$$\begin{cases} c_4(a,b) = -2^4 3^2 ab, \\ c_6(a,b) = 2^5 3^3 (a^3 - b^3), \\ \Delta(a,b) = -2^4 3^3 p^{2\alpha} c^{2n}. \end{cases}$$

It is not too difficult, via Tate's algorithm, to determine the conductor $N_{E_{a,b}}$ of $E_{a,b}$ (for more details, the reader is directed to [16]). We designate by $\mathcal{R}$ the product of the prime numbers distinct from 2, 3, and p that divide c, *i.e.*, the largest squarefree integer prime to $6p$ dividing c. Given an integer k and a prime number l, we denote by $v_l(k)$ the exponent of l in the decomposition of k into prime factors.

Lemma 2.1. *We have (under conditions* (3) *on a, b, and c)*

$$N_{E_{a,b}} = \begin{cases} 18\,p\,\mathcal{R} & \text{if } c \text{ even}, b \equiv -1 \pmod 4, \\ 36\,p\,\mathcal{R} & \text{if } c \text{ odd}, v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4, \\ 72\,p\,\mathcal{R} & \text{if } c \text{ odd}, v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4. \end{cases}$$

In particular, since a and b are coprime, we have that $E_{a,b}$ has multiplicative reduction at p.

Let us denote by

$$\rho_n^{a,b} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n),$$

the canonical mod n Galois representation on $E_{a,b}[n]$, the subgroup of n-torsion points of $E_{a,b}(\overline{\mathbb{Q}})$. It is easy to see that $\rho_n^{a,b}$ has weight 2 (in the sense of [20]). Let $N(\rho_n^{a,b})$ denote the conductor of $\rho_n^{a,b}$, as defined in Serre [20]. Before we proceed further, we will deduce Theorem 1.2 in case $n \mid \alpha$. Following the arguments of Kraus [12], we find that

$$n \mid p + 1 \pm a_p,$$

where a_p is the p-th Fourier coefficient of an elliptic curve over $\mathbb{Q}$ of conductor 72. It follows that $n \leq p + 1 + 2\sqrt{p}$, contradicting $n \geq p^{2p}$. We will thus suppose, from now on, that n does not divide α.

Lemma 2.2. *The following statements hold:*

(a) $N(\rho_n^{a,b}) = N_{E_{a,b}}/\mathcal{R}$.

(b) *The representation $\rho_n^{a,b}$ is irreducible.*

Proof. (a) Let q be a prime distinct from $2, 3, p$ and n. The curve $E_{a,b}$ is readily shown to have multiplicative reduction at q (Lemma 2.1) and the exponent of q in the minimal discriminant of $E_{a,b}$ is a multiple of n. This assertion then follows as a direct consequence of Lemma 2.1 and, essentially, a result of Serre ([20], p.120).

(b) If $\rho_n^{a,b}$ were reducible, since $E_{a,b}$ has a point of order 2, there would exist a subgroup of $E_{a,b}(\mathbb{Q})$ of order $2n$ stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This contradicts the fact that, for $n \geq 11$, the modular curve $Y_0(2n)$ has no $\mathbb{Q}$-rational points (see [10] and [15]). □

Given a positive integer N, we let $S_2(\Gamma_0(N))$ denote the $\mathbb{C}$-vector space of cuspidal modular forms of weight 2 for the congruence subgroup $\Gamma_0(N)$. Denote by $S_2^+(N)$ the subspace of newforms of $S_2(\Gamma_0(N))$, and $g_0^+(N)$ its dimension as a $\mathbb{C}$-vector space. See [14] for an explicit determination of $g_0^+(N)$.

Since the representation $\rho_n^{a,b}$ is irreducible of weight 2 and $E_{a,b}$ is modular (via *e.g.* [5]), there exists a newform $f \in S_2^+(N(\rho_n^{a,b}))$ whose Taylor expansion is

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

and a place $\mathcal{N}$ of $\overline{\mathbb{Q}}$ lying above n, such that for all prime numbers l not dividing $nN_{E_{a,b}}$ one has

$$a_l(f) \equiv a_l(E_{a,b}) \pmod{\mathcal{N}}.$$

It follows that

$$n \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a_l(f) - a_l(E_{a,b})), \tag{5}$$

where K_f denotes the field of definition of the coefficients. Similarly, we have

$$n \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a_l(f) \pm (l+1)), \tag{6}$$

for each prime $l \neq n$ dividing $\mathcal{R}$.

3. Proof of Theorem 1.2

We now proceed with the proof of Theorem 1.2. Let us suppose that f is a weight 2 and level N cuspidal newform (with trivial character), where

$$N \in \{18p, 36p, 72p\},$$

corresponding to a nontrivial solution to equation (2). If $[K_f : \mathbb{Q}] > 1$ then, by Lemme 1 of [11], there exists a prime l satisfying, in all cases, $l \leq 24(p+1)$, and for which $a_l(f) \notin \mathbb{Z}$. Since we have normalized f, the Fourier coefficients $a_2(f), a_3(f)$ and $a_p(f)$ are all in $\{0, \pm 1\}$, whereby $l \notin \{2, 3, p\}$. From the fact that $a_l(E_{a,b})$ is a rational integer satisfying $|a_l(E_{a,b})| \leq 2\sqrt{l}$ while, for any embedding $\sigma : K_f \to \mathbb{R}$ we have $|\sigma(a_l(f)| \leq 2\sqrt{l}$, in each of the cases (5) or (6), the right-hand side is necessarily nonzero and hence

$$n \leq \left(l + 1 + 2\sqrt{l}\right)^{[K_f:\mathbb{Q}]} \leq \left(\sqrt{l} + 1\right)^{2g_0^+(N)}.$$

Applying Theorem 1 of [14], we obtain

$$g_0^+(N) \leq \begin{cases} p & \text{if } N = 18p, 36p, \\ 5p/4 & \text{if } N = 72p, \end{cases}$$

whereby

$$n \leq \left(\sqrt{24(p+1)} + 1\right)^{5p/2}.$$

For $p \geq 211$ a simple exercise in calculus immediately implies that $n < p^{2p}$. Since we may assume that $p = 197$ or $p \geq 317$, it remains to handle the former case. Here, the

(very) slightly sharper inequality $g_0^+(N) \leq 5(p-1)/4$ suffices to imply $n < p^{2p}$ and hence, as desired, a contradiction.

We may thus suppose that the form f has rational integer Fourier coefficients $a_m(f)$ for all $m \geq 1$, whereby f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor $N = 18p$, $36p$ or $72p$. Applying Proposition 2 of Appendice II of Kraus [11], we find that one of the following necessarily occurs:

(i) There exists a prime $l \leq 24(p+1)$, coprime to $6p$, with $a_l(f) \equiv 1 \pmod 2$.

(ii) $a_l(f) \equiv 0 \pmod 2$ for all primes l coprime to $6p$.

In the former case, since n divides the (nonzero) integer $a_l(f) - a_l(E_{a,b})$, we have that

$$n \leq l + 1 + 2\sqrt{l} \leq 24(p+1) + 1 + 4\sqrt{6(p+1)} < p^{2p},$$

where the last inequality is valid for $p \geq 3$. In case (ii), there exists an elliptic curve F, in the given isogeny class, with a rational 2-torsion point. That is, F is an elliptic curve over $\mathbb{Q}$ with 2-torsion and conductor $18p$, $36p$ or $72p$. It follows that $p \in S$, contrary to our earlier assumptions. This completes the proof of Theorem 1.2.

4. Classifying elliptic curves

If an elliptic curve possesses a rational torsion point or isogeny, then its discriminant splits into at least two factors, as a polynomial in its coefficients. Together with the assumption that the curve has bad reduction at only a few primes, this leads us to a number of Diophantine equations which, if lucky, we may be able to solve. This is the approach Hadano [9] takes to classify elliptic curves with certain specified reduction and nontrivial rational torsion. In the example we have in mind, we will however, consider a case rather more general than that treated in [9], though we restrict our attention to rational 2-torsion. For such $E/\mathbb{Q}$, we may suppose that

$$E \ : \ y^2 = x^3 + Ax^2 + Bx,$$

so that the assumption that N_E is divisible by no primes outside $\{2, 3, p\}$ leads us to the conclusion that

$$\Delta_E = 2^4 B^2 (A^2 - 4B) = \pm 2^\alpha 3^\beta p^\gamma,$$

and hence to equations of the shape

$$A^2 = \left| 2^{\alpha_0} 3^{\beta_0} p^{\gamma_0} \pm 2^{\alpha_1} 3^{\beta_1} p^{\gamma_1} \right|.$$

To proceed, one combines case-by-case analysis with assorted tricks of the Diophantine trade; the reader is directed to the relevant sections of [16] for details. The results we quote here follow from combining Theorems 3.13, 3.14 and 3.15 with Lemmata 4.7 – 4.11 of [16], and appealing to the main results of Luca [13]. In what follows, we let $l(n)$ denote the least prime divisor of an integer $n > 1$.

Proposition 4.1. *Let $p > 3$ be prime. Then there exists an elliptic curve $E/\mathbb{Q}$ of conductor $18p$ and having at least one rational point of order 2 precisely when at least one of the following occurs :*

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

$$p = 2^a 3^b \pm 1; \tag{7}$$

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

$$p = \left| 3^b \pm 2^a \right|; \tag{8}$$

(c) *there exist integers* $a \geq 7$, $b \geq 0$ *and* t *such that*

$$p = \left| t^2 \pm 2^a 3^b \right|; \tag{9}$$

(d) *there exist integers* $a \geq 7$, $b \geq 0$ *and* t *such that*

$$3^b\, p = t^2 + 2^a; \tag{10}$$

(e) *there exist integers* $a \geq 7$ *and* t *such that*

$$p = \left| 3t^2 \pm 2^a \right|. \tag{11}$$

Proposition 4.2. *Let* $p > 3$ *be prime. Then there exists an elliptic curve* $E/\mathbb{Q}$ *of conductor* $36p$ *and having at least one rational point of order* 2 *precisely when at least one of the following occurs :*

(a) *there exist integers* t *and* b*, where* $b \geq 0$ *is even, and*

$$p = t^2 + 4 \cdot 3^b; \tag{12}$$

(b) *there exist integers* n, t *and* b*, where* $b \geq 1$ *is odd,* $n = 1$ *or* $l(n) \geq 7$*, and*

$$p^n = \left| t^2 - 4 \cdot 3^b \right|; \tag{13}$$

(c) *there exist integers* t *and* b*, where* $b \geq 1$ *is odd, and*

$$4p = t^2 + 3^b, \tag{14}$$

where $p \equiv -1 \pmod 4$*;*

(d) *there exist integers* t *and* $n \in \{1, 2\}$ *such that*

$$4p^n = 3t^2 + 1 \tag{15}$$

where $p \equiv 1 \pmod 4$*;*

(e) *there exists an integer* t *such that*

$$p = 3t^2 - 4. \tag{16}$$

Proposition 4.3. *Let* $p > 3$ *be prime. Then there exists an elliptic curve* $E/\mathbb{Q}$ *of conductor* $72p$ *and having at least one rational point of order* 2 *precisely when* $p = 29$ *or at least one of the following occurs :*

(a) *there exists an odd integer* b *such that*

$$4p = 3^b + 1; \tag{17}$$

(b) *there exist integers* t *and* b*, where* $b \geq 1$ *is odd, and*

$$p = t^2 + 4 \cdot 3^b; \tag{18}$$

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

$$p = 2^a 3^b \pm 1; \tag{19}$$

(d) *there exist integers* $a \in \{4,5\}$, $b \geq 0$, t *and* $n = 1$ *or* $l(n) \geq 7$, *such that*

$$p^n = \left| t^2 \pm 2^a 3^b \right|; \tag{20}$$

(e) *there exist integers* t *and* b, *where* $b \geq 1$ *is odd, and*

$$4p = t^2 + 3^b, \tag{21}$$

where $p \equiv 1 \pmod 4$*;*

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

$$p = 3^b \pm 2^a; \tag{22}$$

(g) *there exist integers* t *and* $n \in \{1,2\}$ *such that*

$$4p^n = 3t^2 + 1; \tag{23}$$

(h) *there exist integers* n, t *and* b, *where* $b \geq 1$ *is odd,* $n = 1$ *or* $l(n) \geq 7$, *and*

$$3^b p^n = t^2 + 32; \tag{24}$$

(i) *there exist integers* $a \in \{4,5\}$ *and* t *such that*

$$p = 3t^2 - 2^a; \tag{25}$$

(j) *there exist integers* $a \in \{2,4,5\}$ *and* t *such that*

$$p = 3t^2 + 2^a. \tag{26}$$

At this juncture, it is appropriate to note that, in Propositions 4.2 and 4.3, the condition $l(n) \geq 7$ can likely be omitted (though we cannot currently prove this); there are no known solutions to the corresponding Diophantine equations.

With these results in hand, it is a relatively straightforward matter to deduce the following.

Corollary 4.4. *If* p *is prime with* $p \equiv 317$ *or* $1757 \pmod{2040}$, *then* $p \notin S$, *i.e., there does not exist an elliptic curve* $E/\mathbb{Q}$ *of conductor* $18p$, $36p$ *or* $72p$, *with a nontrivial rational* 2*-torsion point.*

Proof. To prove this, we note that Propositions 4.1, 4.2 and 4.3 together with some elementary calculations imply that primes p for which there exists an elliptic curve $E/\mathbb{Q}$ of conductor $18p$, $36p$ or $72p$, with at least one nontrivial rational 2-torsion point, necessarily satisfy $p \not\equiv 77 \pmod{120}$, unless we have one of

$$p = 2^a - 3t^2 \text{ with } a \geq 7, a \equiv 1 \pmod 4 \text{ and } 5 \mid t, \text{ or} \tag{27}$$

$$p^n = t^2 + 4 \text{ with } n \equiv 3 \pmod 4, \text{ or} \tag{28}$$

$$4p^2 = 3t^2 + 1, \tag{29}$$

where t is an integer. In this last case, since positive integer solutions (T, U) to the Diophantine equation $T^2 - 3U^2 = 1$ have $T \equiv 1, 2 \pmod 5$, any p satisfying (29) must be such that $p \equiv 1, 3 \pmod 5$. For equation (28), an old result of Nagell [17] implies that the only positive integral solutions to $t^2 + 4 = y^n$ with $n \geq 3$ are with $t = 2$ and $t = 11$, whereby $p = 5$.

It remains to treat (27). Here, it is easy to check that, since $a \equiv 1 \pmod 4$, we have

$$p = 2^a - 3t^2 \not\equiv \pm 6 \pmod{17}.$$

It follows, as claimed, that $p \not\equiv 317$ or $1757 \pmod{2040}$. □

5. Bounding S

We will now proceed with the proof of Theorem 1.3. Let S_k denote the set of primes p satisfying equation (k) for $k \in \{7, \ldots, 26\}$, so that

$$S = \bigcup_{k=7}^{26} S_k.$$

Define $\pi_{S_k}(x) = \#\{p \leq x : p \text{ prime}, p \in S_k\}$. We will deduce upper bounds for each $\pi_{S_k}(x)$; it is perhaps interesting to note that, in each case, we will in fact bound the integers p satisfying equation (k) for $k \in \{7, \ldots, 26\}$, without appealing to the primality of p.

Before we start, let us take care of the cases where $n > 1$ in (13), (15), (20), (23) and (24). Indeed, if p, n, a, b, t satisfy one of these equations then Shorey and Tijdeman ([21], page 180) implies that n is bounded by an absolute constant, and Darmon and Granville ([8], Theorem 2) implies there are only finitely many solutions for p, n, a, b, t. If $n = 2$ in (23), then p is a term in a (fixed) binary recurrence sequence (and hence there are $\ll \log x$ such primes $p \leq x$). We will suppose, henceforth, that $n = 1$. Under this assumption, it is almost immediate that

$$\pi_{S_k}(x) \ll \sqrt{x} \log^2 x \text{ for } k \in \{7, 12, 14, 15, 16, 17, 18, 19, 21, 23, 25, 26\}$$

and that like inequalities obtain for primes p in (8), (9), (11), (20) and (22) with corresponding $+$ rather than $-$ signs. To see this in case, by way of example, $k = 12$, note that $t^2 + 4 \cdot 3^b \leq x$ implies that $t \leq \sqrt{x}$ and $b \leq \log x$, so that the number of integers of the form $t^2 + 4 \cdot 3^b$ up to x (never mind primes) is at most $\sqrt{x} \log x$. Our weakest upper bound here corresponds to the $+$ case of (9).

It remains to count primes of the shape

$$p = \left|3^b - 2^a\right|, \tag{30}$$

$$p = \left|t^2 - 2^a 3^b\right|, \tag{31}$$

$$p = \left|3t^2 - 2^a\right|, \tag{32}$$

and

$$p = \frac{t^2 + 2^a}{3^b}. \tag{33}$$

Let us begin with (30) and suppose that we have

$$\left|3^b - 2^a\right| \leq x.$$

We appeal to a result of Tijdeman.

Theorem 5.1. ([22, Theorem 1]) *Let A and B be positive integers with $3 < A < B$ and let r and p denote the number of distinct prime factors and the greatest prime factor of AB, respectively. Then*

$$B - A > \frac{A}{(\log A)^{C_1}},$$

where $\log C_1 = r^4\, c_1 + 14r^2 \log\log p$, with c_1 an effectively computable absolute constant.

This result, with $(A, B) = (2^a, 3^b)$ or $(3^b, 2^a)$, implies the existence of an effectively computable positive constant κ such that

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

at least provided that $b > 2$ (if $b \leq 2$, an upper bound of order $\log x$ upon a is immediate). It follows that $3^b\, b^{-\kappa} < x$ and so $b \ll \log x$. Since $|3^b - 2^a| \leq x$, we thus have $2^a < x^\tau$ for some absolute positive constant τ, whereby $\max\{a, b\} \ll \log x$. We may thus conclude that

$$\pi_{S_k}(x) \ll \log^2(x) \ \text{ for } \ k \in \{8, 22\}.$$

To treat primes of the shape (31), we write $a = 2\alpha + \delta_0$ and $b = 2\beta + \delta_1$, where $\delta_i \in \{0, 1\}$. If both a and b are even, *i.e.*, if $\delta_0 = \delta_1 = 0$, then

$$p = |t - 2^\alpha 3^\beta||t + 2^\alpha 3^\beta|,$$

whence

$$p = 2^{\alpha+1}3^\beta \pm 1.$$

The number of such primes up to x is $\ll \log^2 x$. If, however, we have

$$(\delta_0, \delta_1) = (1, 0), (0, 1) \text{ or } (1, 1),$$

then $p \leq x$ implies that

$$\left|\sqrt{2^{\delta_0}3^{\delta_1}} - \frac{t}{2^{\alpha_0}3^{\beta_0}}\right| < \frac{x}{2^{\alpha_0}3^{\beta_0}\left(|t| + 2^{\alpha_0}3^{\beta_0}\right)} < \frac{x}{\left(2^{\alpha_0}3^{\beta_0}\right)^2}.$$

Besides this, a classic result of Ridout [18] (a p-adic version of Roth's theorem) implies, given a nonsquare positive integer d and $\epsilon > 0$, the existence of a positive constant $c(\epsilon)$ such that if α_0, β_0 and t are nonnegative integers then

$$\left|\sqrt{d} - \frac{t}{2^{\alpha_0}3^{\beta_0}}\right| > \frac{c(\epsilon)}{(2^{\alpha_0}3^{\beta_0})^{1+\epsilon}}. \tag{34}$$

Applying this with $d \in \{2, 3, 6\}$ and, say, $\epsilon = 1/2$ yields the inequality

$$\max\{\alpha_0, \beta_0\} \ll \log x$$

and so the number of primes of the shape (31) up to x is $O(\sqrt{x}\log^2 x)$, as desired. A similar argument (applying (34) with $d \in \{3, 6\}$) implies that the corresponding number of primes of the form (32) is $O(\sqrt{x}\log x)$.

It remains to treat primes of the shape (33); we will show that the number of such primes is $O(\sqrt{x}\log x)$. Here, we must argue somewhat more carefully. We begin by noting that if $(t^2 + 2^a)/3^b \leq x$ is an integer (where a, b and t are positive integers), then

$$2^a < t^2 + 2^a \leq 3^b x,$$

whereby

$$a \leq \frac{\log(3^b x)}{\log 2} \ll b + \log x. \tag{35}$$

Fix a and b. Then the congruence

$$t^2 + 2^a \equiv 0 \pmod{3^b}$$

has exactly 2 solutions modulo 3^b. Call these least positive solutions t_1 and t_2, so that $t = t_j + 3^b\lambda$ for some $j \in \{1, 2\}$ and $\lambda \geq 0$. Then

$$\frac{t^2 + 2^a}{3^b} = \frac{t_j^2 + 2^a}{3^b} + 2t_j\lambda + 3^b\lambda^2 \leq x$$

and so $3^b\lambda^2 < x$, whereby $\lambda \leq x^{1/2}/3^{b/2}$. Thus, for a and b fixed, the number of such positive integers t is at most

$$\frac{2\,x^{1/2}}{3^{b/2}} + 2. \tag{36}$$

Our goal will be to show that

$$b \ll \log x. \tag{37}$$

If this inequality is satisfied, then (35) implies that also $a \ll \log x$. Thus, summing (36) over all the values of a once b is fixed, then over b, we find that the number of integers of the shape $\frac{t^2+2^a}{3^b}$ which are less than or equal to x and satisfy (37) is

$$O\left(x^{1/2}\log x\left(\sum_{b=1}^{\infty}\frac{1}{3^{b/2}}\right) + \log^2 x\right)$$

and hence $\ll x^{1/2}\log x$, as desired.

We will suppose, then, that $\kappa > 4 \times 10^7$ is a (large) positive constant to be specified later, and that there exists an integer of the form $\frac{t^2+2^a}{3^b}$ which is less than or equal to x and satisfies

$$b > \kappa \log x. \tag{38}$$

We wish to deduce a contradiction. Begin by writing

$$t^2 + 2^a = 3^b m$$

for positive integers m and b. Since 3 divides $t^2 + 2^a$, it follows that a is odd, say $a = 2a_1 + 1$. Factoring the above equation in $\mathbb{Z}[i\sqrt{2}]$ (which has class number one), we readily conclude that

$$t + i\sqrt{2} \cdot 2^{a_1} = \alpha^b m_1, \tag{39}$$

where $m_1 = u + i\sqrt{2}v$ is such that u and v are integers with $u^2 + 2v^2 = m$, and α is one of $1 \pm i\sqrt{2}$. Conjugating (39) and eliminating t we find that

$$i\sqrt{2} \cdot 2^{a_1} = \alpha^b m_1 - \beta^b n_1, \tag{40}$$

where $\beta = \overline{\alpha}$ and $n_1 = \overline{m_1}$. We will exploit relation (40) in two different ways.

On the one hand, we compute the 2-adic valuation of both sides of relation (40). From the left-hand side, it is greater than or equal to $a/2$. On the other hand, from the right-hand side, it equals

$$\nu_2(\alpha^b m_1 - \beta^b n_1) = \nu_2((\alpha/\beta)^b (m_1/n_1) - 1),$$

where we use the fact that β and n_1 have odd norms in $\mathbb{Q}[i\sqrt{2}]$. Putting $\gamma = \alpha/\beta$ and $\delta = m_1/n_1$, we apply a lower bound for linear forms in 2-adic logarithms due to Bugeaud and Laurent ([6], Théorème 4) with, in the notation of that paper, $\mu = 10$ and $\nu = 5$. We deduce the inequality

$$\nu_2((\alpha/\beta)^b (m_1/n_1) - 1) < 3656 \log^2 \left(\frac{b}{\log x} \right) \log x.$$

Here, we have used the fact that the absolute logarithmic height of γ is $\log 3$, while that of δ is $\log(m_1 n_1)/2 = \log m \leq \log x$. Thus we may conclude that

$$a < 7312 \log^2 \left(\frac{b}{\log x} \right) (\log x).$$

If $a > (\log \kappa)^{-1} b$, it follows that

$$\frac{\frac{b}{\log x}}{\log^2 \left(\frac{b}{\log x} \right)} < 7312 \log \kappa,$$

whereby, from (38),

$$\kappa < 7312 \log^3 \kappa,$$

contradicting $\kappa > 4 \times 10^7$.

We may thus assume that

$$a \leq (\log \kappa)^{-1} b. \tag{41}$$

Next, we apply Schmidt's Subspace Theorem [19] to equation (40). Let $K = \mathbb{Q}[i\sqrt{2}]$. We take $\mathcal{S} = \{\alpha, \beta, \infty\}$ as normalized valuations over K. Put $\mathbf{x} = (x_1, x_2)$. For $j = 1, 2$ and $\nu \in \mathcal{S}$, we take $L_{j,\nu}(\mathbf{x}) = x_j$ for all $(j, \mu) \in \{1, 2\} \times \mathcal{S}$ except for $(j, \mu) = (2, \infty)$ for which we take $L_{2,\infty}(\mathbf{x}) = x_1 - x_2$. Next we compute

$$\prod_{(j,\mu) \in \{1,2\} \times \mathcal{S}} |L_{j,\mu}(\mathbf{x})|_\mu, \tag{42}$$

where $\mathbf{x} = (x_1, x_2) = (\alpha^b m_1, \beta^b m_2)$. Obviously

$$\prod_{\mu \in \mathcal{S}} |L_{1,\mu}(\mathbf{x})|_\mu = \prod_{\mu \in \mathcal{S}} |x_1|_\mu = |m_1|.$$

Furthermore,

$$\prod_{\mu \in \mathcal{S} \setminus \{\infty\}} |L_{2,\mu}(\mathbf{x})|_\mu = |x_2|_\alpha |x_2|_\beta = 3^{-b/2}.$$

Finally, $|L_{2,\infty}(\mathbf{x})| = |x_1 - x_2| = 2^{a/2}$. Thus, the double product appearing in (42) is bounded by

$$\frac{|m_1| 2^{a/2}}{3^{b/2}} \leq \frac{x^{1/2} 2^{a/2}}{3^{b/2}}.$$

From (41), it follows that $2^{a/2} \leq 3^{b/4}$, and hence

$$\prod_{(j,\mu) \in \{1,2\} \times \mathcal{S}} |L_{j,\mu}(\mathbf{x})|_\mu \leq \frac{x^{1/2}}{3^{b/4}} < 3^{-b/8},$$

where the last inequality is a consequence of (38). Noting that

$$|x_1| = |x_2| \leq 3^{b/2} x \leq 3^b$$

(via (38)), we conclude that

$$\prod_{(j,\mu) \in \{1,2\} \times \mathcal{S}} |L_{j,\mu}(\mathbf{x})|_\mu \ll \frac{1}{(\max\{|x_1|, |x_2|\})^{1/8}}.$$

The Subspace Theorem [19] asserts that in this case there exist finitely many pairs $(c_i, d_i) \in K^2 \setminus \{(0,0)\}$, with $i = 1, \ldots, s$, such that all solutions $\mathbf{x}$ of (40) satisfy $c_i x_1 = d_i x_2$ for some $i = 1, \ldots, s$. We may assume that c_i and d_i are coprime. For a fixed i, this relation implies that $\alpha^b \mid d_i \beta^b n_1$, and since α and β are coprime, that $\alpha^b \mid d_i n_1$. Since $|n_1| \leq \sqrt{x}$, choosing κ suitably large (relative to $\max |d_i|$), this contradicts (38). This completes the proof of Theorem 1.3.

6. Extending Theorem 1.2

We can, in fact, strengthen Theorem 1.2 substantially, so that its conclusion applies to many primes $p \in S$. To see how this is achieved, we begin by noting that the Frey curve constructed in (4) provides us with somewhat more information than just the existence of a nontrivial rational 2-torsion point. Indeed, the curve is of the form $y^2 = f(x)$, where

$$f(x) = (x - b + a)(x^2 + (a - b)x + (a^2 + ab + b^2)).$$

This last quadratic has discriminant $-3(a+b)^2$ and hence f splits completely modulo l for $l \geq 5$ prime, precisely when $\left(\frac{-3}{l}\right) = 1$; *i.e.*, for $l \equiv 1 \pmod 6$. For each such l, we thus have

$$a_l(E_{a,b}) \equiv l + 1 \pmod 4. \tag{43}$$

For each $p \in S$, there exists (by definition) at least one $E/\mathbb{Q}$ with conductor in $\{18p, 36p, 72p\}$ and $2 \mid \#E(\mathbb{Q})_{\text{tors}}$. Besides, it might be that there are no such curves with $4 \mid \#E(\mathbb{Q})_{\text{tors}}$. In such a case, then, there is a chance that (43), in conjunction

with (5) and (6), might imply that equation (2) has no nontrivial solutions for suitably large prime n.

A short computation reveals that the following $p \in S$, with $p < 197$, have the property that every $E/\mathbb{Q}$ with conductor in $\{18p, 36p, 72p\}$ has at most a single rational torsion point of exact order 2 :

$$79, 83, 103, 149, 151, 157, 163, 167, 173, 181$$

(indeed, one may show that this is true of "most" elements of S). From this list, the primes $p = 83, 149, 167$ and 173 have the property that every $E/\mathbb{Q}$ of conductor $18p, 36p$ and $72p$ has at least one corresponding prime $l \equiv 1 \pmod 6$ for which $a_l(E) \not\equiv l + 1 \pmod 4$. Arguing carefully (and computing Fourier coefficients of modular forms via, say, `Magma`), we can prove, for instance, a result of the following flavour.

Proposition 6.1. *The equation*

$$x^3 + y^3 = 83^\alpha z^n$$

has no solutions in coprime nonzero integers x, y and z, integer $\alpha \geq 1$ and prime $n \geq 17$.

It is not too difficult to classify the elements of S for which we may apply these arguments, but we will not undertake this here.

Acknowledgements. M. Bennett was supported in part by a grant from NSERC. F. Luca was supported in part by grants SEP-CONACyT 79685 and PAPIIT 100508.

REFERENCES

[1] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, preprint.

[2] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, preprint.

[3] B. Bektemirov, B. Mazur, W. Stein and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 2, 233–254.

[4] M. A. Bennett and J. Mulholland, *Elliptic curves with prescribed reduction and nontrivial torsion*, in preparation.

[5] 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), no. 4, 843–939.

[6] Y. Bugeaud and M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory **61** (1996), no. 2, 311-342.

[7] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra **322** (2009), no. 3, 638–656.

[8] H. Darmon and A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.

[9] T. Hadano, *Elliptic curves with a rational point of finite order*, Manuscripta Math. **39** (1982), no. 1, 49–79.

[10] M. A. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202.

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

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

[13] F. Luca, *On the equation $x^2 + 2^a \cdot 3^b = y^n$*, Int. J. Math. Math. Sci. **29** (2002), no. 4, 239–244.

[14] G. Martin, *Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$*, J. Number Theory **112** (2005), no. 2, 298–331.

[15] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978).

[16] J. T. Mulholland, *Elliptic curves with rational 2-torsion and related ternary Diophantine equations*, Ph. D. Thesis, U. of British Columbia (Canada), 2006, 324 pp.

[17] T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk. Mat. Forensings Skrifter **13** (1923), 65–82.

[18] D. Ridout, *Rational approximations to algebraic numbers*, Mathematika **4** (1957), 125–131.

[19] W. M. Schmidt, *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics **1467**, Springer-Verlag, Berlin, 1991, viii+217 pp.

[20] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*, Duke Math. J. **54** (1987), no. 1, 179–230.

[21] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, 1986.

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

M. A. BENNETT, DEPT. OF MATH., U. OF BRITISH COLUMBIA, VANCOUVER, B.C., V6T 1Z2, CANADA.
bennett@math.ubc.ca

F. LUCA, MATHEMATICAL INSTITUTE, UNAM AP. POSTAL 61-3 (XANGARI), CP 58089 MORELIA, MICHOACAN, MEXICO.
fluca@matmor.unam.mx

J. MULHOLLAND, DEPT. OF MATH., SIMON FRASER U., BURNABY, B.C., V5A 1S6, CANADA.
jtmulhol@math.sfu.ca