C. R. Math. Rep. Acad. Sci. Canada Vol. **28**, (1), 2006 pp. 6–11

ON THE DIOPHANTINE EQUATION $x^n + y^n = 2^\alpha pz^2$

Dedicated to the memory of Professor Vishwa Dumir

MICHAEL A. BENNETT AND JAMIE MULHOLLAND

Presented by David Boyd, FRSC

ABSTRACT. We show, if p is prime, that the equation $x^n + y^n = 2pz^2$ has no solutions in coprime integers x, y and z with $|xy| > 1$ and prime $n > p^{27p^2}$, and, if $p \neq 7$, the equation $x^n + y^n = pz^2$ has no solutions in coprime integers x, y and z with $|xy| > 1$, z even and prime $n > p^{3p^2}$.

RÉSUMÉ. Nous montrons que, si p est premier, l'équation $x^n + y^n = 2pz^2$ n'a pas de solution parmi les nombres entiers copremiers x, y, z, avec $|xy| > 1$ et $n > p^{27p^2}$ premier. Nous montrons aussi que, si $p \neq 7$, l'équation $x^n + y^n = pz^2$ n'a pas de solution parmi les nombres entiers copremiers x, y, z, avec $|xy| > 1$, z pair, et $n > p^{3p^2}$ premier.

1. Introduction.

In the years following Wiles' [15] proof of Fermat's Last Theorem, there has arisen a substantial body of work on solving more general ternary Diophantine equations of the shape

$$Ax^p + By^q = Cz^r, \tag{1}$$

via similar techniques, based on the modularity of Galois representations. The reader is directed to [5], [9] and [12] for survey articles, and to [2] and [4] for relatively recent developments. In this short note, we will restrict our attention to families of triples (A, B, C) for which (1) may be shown to be unsolvable for all suitably large primes n, where $(p, q, r) = (n, n, 2)$. We prove the following.

THEOREM 1.1. *Let $p \neq 7$ be prime and $\alpha \geq 1$ be an integer. Then the equation*

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

has no solutions in coprime nonzero integers x, y and z, and prime n satisfying $n > p^{27p^2}$.

As an almost immediate consequence of this, we have:

COROLLARY 1.2. *Let $p \neq 7$ be prime. Then equation* (2) *has at most finitely many solutions in coprime nonzero integers x, y and z, and integers $\alpha \geq 1$, $n \geq 5$.*

Received by the editors on March 1, 2006.
The authors were supported in part by NSERC grant DG80969.
AMS subject classification: 11D41, 11G05.

We note that our techniques may also be used to treat the case $p = 7$, if α is additionally assumed to be odd. Similarly general conclusions for equations such as those of the shape

$$x^n + p^\alpha y^n = z^2$$

have been obtained by Ivorra and Kraus [7] using a classification [6] of elliptic curves over $\mathbb{Q}$ with rational 2-torsion and multiplicative reduction at a single odd prime. The case at hand is essentially the additive reduction analogue of these results.

2. **From elliptic curves to modular forms.** Let us suppose, here and henceforth, that $n \geq 7$ is an odd prime, and that (a, b, c) are coprime nonzero integers satisfying

$$a^n + b^n = 2^\beta pc^2, \tag{3}$$

where $\beta \in \{0, 1\}$ and, in case $\beta = 0$, c is even and, without loss of generality, $b \equiv -p \pmod 4$. As in [1], we associate to the solution (a, b, c) an elliptic curve

$$E = E_\beta(a, b, c)\colon Y^2 = X^3 + 2^{\beta+1}cpX^2 + 2^\beta pb^n X$$

with corresponding mod n Galois representation

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

on the n-torsion $E[n]$ of E. Via Lemmata 3.2 and 3.3 of [1], this representation arises from a cuspidal newform f of weight 2, trivial Nebentypus character, and level $32p^2$ (if $\beta = 0$) or $256p^2$ (if $\beta = 1$).

To prove Theorem 1.1, it remains to show that the modular forms under discussion here cannot, in fact, give rise to ρ_n^E. The following three results from [1] provide us with the means to eliminate forms from consideration. The first proposition enables us to discount the possibility of f being of dimension greater than one, at least for large enough n. It is from this result that we derive the stated lower bound for n in our theorem.

PROPOSITION 1. *Suppose $n \geq 7$ is prime and $E = E_\beta(a, b, c)$ is as given previously. Suppose further that*

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

is a newform of weight 2 and level N giving rise to ρ_n^E and that K_f is a number field containing the Fourier coefficients of f. If q is a prime, coprime to $2pn$, then n divides one of either

$$\mathrm{Norm}_{K_f/\mathbb{Q}}\big(c_q \pm (q+1)\big)$$

or

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

for some integer $0 \le r \le \sqrt{q}$.

The following pair of results will prove crucial in eliminating one-dimensional forms from consideration.

PROPOSITION 2. *Suppose* $n \ge 7$ *is prime with* $n \ne p$, *and that* $E = E_\beta(a,b,c)$ *is as given previously. 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* p.

PROPOSITION 3. *Suppose* $n \ge 7$ *is prime and* $E = E_\beta(a,b,c)$ *is as given previously. Suppose that* ρ_n^E *arises from a newform having CM by an imaginary quadratic field* K. *Then either* ab *is even or* $n \le 13$.

3. **Elliptic curves with rational 2-torsion.** To apply the previous results, we need to understand one-dimensional weight 2 cuspidal newforms of level $N = 32p^2$ or $256p^2$. These correspond to elliptic curves over $\mathbb{Q}$ of conductor $32p^2$ or $256p^2$. The second author [14] has provided a classification of such curves, provided they possess at least one rational 2-torsion point. We restate the relevant results in the following two propositions.

PROPOSITION 4. *Suppose* $p \ge 5$ *is prime and that* $E/\mathbb{Q}$ *is an elliptic curve with a rational* 2*-torsion point and conductor* $32p^2$. *Then* E *is isogenous over* $\mathbb{Q}$ *to a curve of the form*

$$y^2 = x^3 + a_2x^2 + a_4x$$

with coefficients given in the following table.

p	a_2	a_4	j*-invariant*
any	0	$-p^2$	1728
any	0	$(-1)^{(p+1)/2}p$	1728
any	0	$(-1)^{(p+1)/2}p^3$	1728
7	± 7	$2{\cdot}7^2$	8000/7
7	± 7	$2{\cdot}7$	-2^6
7	$\pm 7^2$	$2{\cdot}7^3$	-2^6
$s^2+1,\ s \in \mathbb{Z}$	$2ps$	$-p^2$	$\frac{64(4p-1)^3}{p}$
$s^2+8,\ s \in \mathbb{Z}$	ps	$-2p^2$	$\frac{64(p-2)^3}{p}$
$s^2-8,\ s \in \mathbb{Z}$	ps	$2p^2$	$\frac{64(p+2)^3}{p}$

PROPOSITION 5. *Suppose $p \geq 5$ is prime and that $E/\mathbb{Q}$ is an elliptic curve with a rational 2-torsion point and conductor $256p^2$. Then E is isogenous over $\mathbb{Q}$ to a curve of the form*

$$y^2 = x^3 + a_2x^2 + a_4x$$

with coefficients given in the following table.

p	a_2	a_4	j-*invariant*
any	0	$\pm 2p$	1728
any	0	$\pm 2p^2$	1728
any	0	$\pm 2p^3$	1728
any	$\pm 4p$	$2p^2$	$2^6 5^3$
23	$\pm 2^3 \cdot 23 \cdot 39$	$2 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$
23	$\pm 2^4 \cdot 23 \cdot 39$	$2^3 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$
$2s^2+1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^3$	$\frac{-64(p-4)^3}{p^2}$
$2s^2+1,\ s \in \mathbb{Z}$	$\pm 4ps$	$-2p^2$	$\frac{64(4p-1)^3}{p}$
$\sqrt{2s^2+1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^4$	$\frac{64(p^2-4)^3}{p^4}$
$\sqrt{2s^2+1},\ s \in \mathbb{Z}$	$\pm 4ps$	$-2p^2$	$\frac{64(4p^2-1)^3}{p^2}$
$2s^2-1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^3$	$\frac{64(p+4)^3}{p^2}$
$2s^2-1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^2$	$\frac{64(4p+1)^3}{p}$
$\sqrt{2s^2-1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^4$	$\frac{64(p^2+4)^3}{p^4}$
$\sqrt{2s^2-1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^2$	$\frac{64(4p^2+1)^3}{p^2}$

The main feature of these propositions we will use is that an elliptic curve $E/\mathbb{Q}$ with rational 2-torsion and conductor $32p^2$ or $256p^2$ either has CM or p dividing the denominator of $j(E)$, with a single exception: there are curves of conductor $32p^2$ when $p = 7$ without CM and potentially good reduction at p, namely

$$y^2 = x^3 \pm 7x^2 + 14x \quad \text{and} \quad y^2 = x^3 \pm 49x^2 + 686x.$$

It is the presence of these curves which prevents us from extending Theorem 1.1 to include $p = 7$.

4. **Proof of Theorem 1.1.** We now proceed with the proof of Theorem 1.1. Let us suppose that f is a weight 2, level N cuspidal newform f (with trivial character), where

$$N \in \{32p^2, 256p^2\},$$

corresponding, as in Section 2, to a nontrivial solution to equation (3). From Theorem 3 of [8], we may suppose that f has rational integer Fourier coefficients,

provided $n \geq p^{3p^2}$ (in case $N = 32p^2$) or $n \geq p^{27p^2}$ (if $N = 256p^2$), where, in either case, we suppose that $p \geq 11$. This follows from the fact that, if we let $g_0^+(N)$ denote the dimension (as a $\mathbb{C}$-vector space) of the space of cuspidal, weight 2, level N newforms, we have, applying Theorem 1 of Martin [11],

$$g_0^+(32p^2) = p^2 - p - 1,$$

and

$$g_0^+(256p^2) = 8p^2 - 10p - 4.$$

To finish the proof of Theorem 1.1, we will combine Propositions 4 and 5 with the Proposition of Appendice II of Kraus and Oesterlé [10] (regarding this last assertion, note the comments in the Appendice of [8]). We define

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

where the product is over prime l.

PROPOSITION 6. (Kraus and Oesterlé) *Let k be a positive integer, χ a Dirichlet character of conductor N and $f = \sum_{n\geq 0} c_n q^n$ be a modular form of weight k, character χ for $\Gamma_0(N)$, with $c_n \in \mathbb{Z}$. Let p be a rational prime. If $c_n \equiv 0 \pmod{p}$ for all $n \leq \mu(N)k/12$, then $c_n \equiv 0 \pmod{p}$ for all n.*

Since the form f has rational integer Fourier coefficients c_n for all $n \geq 1$, f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor $N = 32p^2$ or $256p^2$. Define

$$f^* = \sum_{\substack{n\geq 1 \\ (n,2p)=1}} c_n q^n \quad \text{and} \quad g^* = \sum_{\substack{n\geq 1 \\ (n,2p)=1}} \sigma_1(n) q^n,$$

where $\sigma_1(n)$ is the usual sum of divisors function; *i.e.*, $\sigma_1(n) = \sum_{d|n} d$. Lemma 4.6.5 of Miyake [13] ensures that f^* and g^* are weight 2 modular forms of level dividing $512p^3$. Applying Proposition 6 (at the prime 2) to $f^* - g^*$ and using the fact that $\sigma(l) = l + 1$, for all primes l, we have either that there exists a prime l, coprime to $2p$, satisfying $l \leq 128p^2(p+1)$ and $c_l \equiv 1 \pmod 2$, or that $c_l \equiv 0 \pmod 2$, for all prime l coprime to $2p$. In the former case, since n divides either the (nonzero) integer $c_l - a_l$ or $c_l \pm (l+1)$, we obtain the inequality

$$n \leq l + 1 + 2\sqrt{l} \leq 128p^2(p+1) + 1 + 16p\sqrt{p+1} < p^p, \tag{4}$$

which is valid for $p \geq 11$. In the latter situation then, a curve in the given isogeny class, say F, necessarily has a rational 2-torsion point. Propositions 4 and 5 then immediately imply, if $p \neq 7$, that F has j-invariant whose denominator is divisible by p, or CM by an order in $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. In the

former case, Proposition 2 provides an immediate contradiction. In the latter, we conclude from Proposition 3 that $n \leq 13$ (since $ab \equiv 1 \pmod 2$). Combining these observations with (4) and simple calculations completes the proofs of Theorem 1.1.

Corollary 1.2 is an easy consequence of Theorem 1.1, after applying a result of Darmon and Granville [3] (which implies, for fixed values of $n \geq 5$, that the equation $x^n + y^n = 2^\alpha pz^2$ has at most finitely many solutions in coprime, nonzero integers x, y and z, and positive integer α).

5. **Concluding remarks.** In case $p \in \{2, 3, 5\}$, equation (2) is solved completely in [1], for $n \geq 4$. Further, the equation

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

with x, y and z coprime nonzero integers, may, as in *e.g.* Krauss [7], be treated for *fixed* values of n. We will not undertake this here.

References

1. M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms.* Canad. J. Math. **56**(2004), 23–54.
2. M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$. Compos. Math. **140**(2004), 1399–1416.
3. 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), 513–543.
4. J. Ellenberg, *Galois representations attached to* $\mathbb{Q}$*-curves and the generalized Fermat equation* $A^4 + B^2 = C^p$. Amer. J. Math. **126**(2004), 763–787.
5. ———, *Q-curves and Galois representation.* In: Modular Curves and Abelian Varieties, Progr. Math. **224**(2004), 93–103.
6. W. Ivorra, *Courbes elliptiques sur* $\mathbb{Q}$*, ayant un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, de conducteur* $2^N p$. Dissertationes Math. (Rozprawy Mat.) **429**(2004).
7. W. Ivorra and A. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$. Canad. J. Math. **58**(2006), 115–153.
8. A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée.* Canad. J. Math. **49**(1997), 1139–1161.
9. ———, *On the equation* $x^p + y^q = z^r$*: a survey.* Ramanujan J. **3**(1999), 315–333.
10. A. Kraus and J. Oesterlé, *Sur une question de B. Mazur.* Math. Ann. **293**(1992), 259–275.
11. G. Martin, *Dimensions of the spaces of cuspforms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$. J. Number Theory, to appear.
12. L. Merel, *Arithmetic of elliptic curves and Diophantine equations.* J. Théor. Nombres Bordeaux **11**(1999), 173–200.
13. T. Miyake, *Modular Forms.*[2pt] Springer–Verlag, Berlin, 1989.
14. J. Mulholland, *Classification of elliptic curves over* $\mathbb{Q}$ *with a rational point of order* 2 *and conductor* $2^n p^2$. Preprint.
15. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math. **141**(1995), 443–551.

Department of Mathematics
University of British Columbia
Vancouver, BC V6T 1Z2
email: bennett@math.ubc.ca
url: http://www.math.ubc.ca/∼bennett

Department of Mathematics
University of British Columbia
Vancouver, BC V6T 1Z2
email: jmulholl@math.ubc.ca
url: http://www.math.ubc.ca/∼jmulholl