ON THE DIOPHANTINE EQUATION $x^n + y^n = 2^\alpha p z^2$.

MICHAEL A. BENNETT AND JAMIE MULHOLLAND

Abstract. We show, if p is prime, that the equation $x^n + y^n = 2pz^2$ has no solutions in coprime integers x and y with $|xy| \geq 1$ and $n > p^{132p^2}$, and, if $p \neq 7$, the equation $x^n + y^n = pz^2$ has no solutions in coprime integers x and y with $|xy| \geq 1$ and $n > p^{12p^2}$.

1. Introduction

In the years following Wiles' [19] 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 [6], [12], [15] and the forthcoming book of Cohen [3] for survey articles, and to [5] and [2] 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 proven unsolvable, for all suitably large prime n, where $(p, q, r) = (n, n, 2)$. We prove the following.

Theorem 1.1. *Let $p \neq 7$ be prime. Then the equation*

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

has no solutions in coprime nonzero integers x and y, positive integers z and α, and prime n satisfying $n > p^{132p^2}$.

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 and y, and positive integers z, α and $n \geq 5$.*

We note that our techniques lead to the same conclusions if $p = 7$, in the case where α is additionally assumed to be odd.

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

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

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

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

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

with corresponding mod n Galois representation

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

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

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

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

$$Norm_{K_f/\mathbb{Q}}\,(c_q \pm (q+1))$$

or

$$Norm_{K_f/\mathbb{Q}}(c_q \pm 2r),$$

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

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

Proposition 2.2. *Suppose $n \geq 7$ is prime with $n \neq p$, 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 2.3. *Suppose $n \geq 7$ 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 one of the following holds:*
(a) *$ab = \pm 2^r$, $r > 0$, $2 \not| ABC$ 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.*

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 [17] 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 3.1. *Suppose $p \geq 5$ 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 3.2. *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

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

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

To prove Theorem 1.1, we will combine Propositions 3.1 and 3.2 with a result of Kraus (Lemme 1 of [10]) and the Proposition of Appendice II of Kraus and Oesterlé [13] (regarding this last assertion, note the comments in the Appendice of [10]). We define

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

where the product is over prime l.

Proposition 4.1. *(Kraus) Let N be a positive integer and $f = \sum_{n \geq 1} c_n q^n$ be a weight 2, level N newform, normalized so that $c_1 = 1$. Suppose that for every prime p with $(p, N) = 1$ and $p \leq \mu(N)/6$ we have $c_p \in \mathbb{Z}$. Then we may conclude that $c_n \in \mathbb{Z}$ for all $n \geq 1$.*

Proposition 4.2. *(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.*

We now proceed with the proofs of Theorem 1.1; as noted earlier, we may assume the existence of a weight 2, level N cuspidal newform f (with trivial character), where

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

If f has at least one Fourier coefficient that is not a rational integer, then, from Proposition 4.1, there is a prime l coprime to $2p$ with

$$l \leq \begin{cases} 8p(p+1) & \text{if } N = 32p^2, \\ 64p(p+1) & \text{if } N = 256p^2. \end{cases} \tag{4}$$

such that $c_l \notin \mathbb{Z}$. It follows from Proposition 2.1 that n divides $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_l - a_l)$, where a_l is the lth Fourier coefficient corresponding to the Frey curve $E_\beta(a, b, c)$. Since $a_l \in \mathbb{Z}$ (whereby $a_l \neq c_l$), and l is coprime to $2p$, the Weil bounds; $|c_\ell| \leq 2\sqrt{\ell}$, $|a_\ell| \leq \ell + 1$, imply that

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

where, as previously, K_f denotes the field of definition for the Fourier coefficients of the form f. Next, we note that $[K_f : \mathbb{Q}] \leq g_0^+(N)$ where $g_0^+(N)$ denotes the dimension (as a $\mathbb{C}$-vector space) of the space of cuspidal, weight 2, level N newforms. Applying Theorem 2 of Martin [14] we have

$$g_0^+(32p^2) \leq \frac{32p^2 + 1}{12} \leq 3p^2,$$

and

$$g_0^+(256p^2) \leq \frac{256p^2 + 1}{12} \leq 22p^2.$$

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

$$n \leq \begin{cases} \left(\sqrt{8p(p+1)}+1\right)^{6p^2} & \text{if } N = 32p^2, \\ \left(\sqrt{64p(p+1)}+1\right)^{44p^2} & \text{if } N = 256p^2. \end{cases} \tag{6}$$

It follows, after routine calculation, that

$$n \leq \begin{cases} p^{12p^2} & \text{if } N = 32p^2, \\ p^{132p^2} & \text{if } N = 256p^2. \end{cases}$$

where these inequalities are a consequence of (6) for $p \geq 5$.

It remains, then, to consider the case when the form f has rational integer Fourier coefficients c_n for all $n \geq 1$. In such a situation, f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor $N = 32p^2$ or $256p^2$. Define

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

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 [16] ensures that f^* and g^* are weight 2 modular forms of level dividing $512p^3$. Applying Proposition 4.2 (at the prime 2) to $f^* - g^*$ and using the fact that $\sigma(l) = l + 1$, for all primes l one of the following necessarily occurs :

(i) There exists a prime l, coprime to $2p$, satisfying $l \leq 128p^2(p+1)$ and $c_l \equiv 1 \pmod 2$.

(ii) $c_l \equiv 0 \pmod 2$ for all prime l coprime to $2p$.

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

$$n \leq l + 1 + 2\sqrt{l} \leq 128p^2(p+1) + 1 + 16p\sqrt{p+1} < p^{2p}, \tag{7}$$

where the last inequality is valid for $p \geq 5$. In the latter situation, then any curve in the given isogeny class, say F, necessarily has a rational 2-torsion point. Propositions 3.1 and 3.2 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 2.2 provides an immediate contradiction. In the latter, we conclude from Proposition 2.3 that $n \leq 13$ (after noting that part (a) of Proposition cannot occur in this case since we are assuming $ab \equiv 1 \pmod 2$). Combining these observations with (7) and the inequalities following (6) 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 [4] (which implies, for fixed values of $n \geq 5$, that the equation $x^n + y^n = 2^\alpha p z^2$ 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 $n \geq 4$. The equation

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

with x, y and z coprime nonzero integers, z even, may, as in e.g [11], be treated for *fixed* values of n.

References

[1] M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, 56 (2004), no. 1, 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. Cohen,

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

[5] 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.

[6] J. Ellenberg,

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

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

[9] W. Ivorra, Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$, preprint.

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

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

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

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

[14] G. Martin, Dimensions of the spaces of cuspforms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$, *J. Number Theory*, to appear.

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

[16] T. Miyake, Modular Forms, Springer Verlag, Berlin 1989, x+335pp.

[17] J.Mulholland, Classification of elliptic curves over $\mathbb{Q}$ with a rational point of order 2 and conductor $2^n p^2$, In preparation.

[18] W. Stein, The Modular forms database, Available from the website `http://modular.fas.harvard.edu/Tables/`, 2005.

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

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

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada

URL: `http://www.math.ubc.ca/∼bennett`

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

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada

URL: `http://www.math.ubc.ca/∼jmulholl`