Bull. Aust. Math. Soc. **82** (2010), 505–510
doi:10.1017/S000497271000033X

ON A CLASS OF GENERALIZED FERMAT EQUATIONS

ANDRZEJ DĄBROWSKI

(Received 22 November 2009)

Abstract

We generalize the main result of the paper by Bennett and Mulholland ['On the diophantine equation $x^n + y^n = 2^\alpha pz^2$', *C. R. Math. Acad. Sci. Soc. R. Can.* **28** (2006), 6–11] concerning the solubility of the diophantine equation $x^n + y^n = 2^\alpha pz^2$. We also demonstrate, by way of examples, that questions about solubility of a class of diophantine equations of type $(3, 3, p)$ or $(4, 2, p)$ can be reduced, in certain cases, to studying several equations of the type $(p, p, 2)$.

2000 *Mathematics subject classification*: primary 11D41; secondary 11F33, 11F80, 11G05.
Keywords and phrases: generalized Fermat equation, elliptic curve, modular form, Galois representation.

1. Introduction

By the work of Hellegouarch, Frey, Serre, Ribet, Wiles, Taylor and many others [5, 13–15], we can reduce the study of a class of ternary diophantine equations (generalized Fermat equations) $Ax^p + By^q = Cz^r$ to modern techniques coming from Galois representations and modular forms. In all known cases, the proofs follow a variant of the method of Frey (or Frey–Hellegouarch) curves and Ribet's level-lowering theorem. We should stress that Frey curves have been constructed for only a few families of diophantine equations. In particular, a number of partial (sometimes complete) results are available when (p, q, r) is one of the following types: (p, p, p), $(p, p, 2)$, $(p, p, 3)$, $(3, 3, p)$, $(4, 4, p)$, $(5, 5, p)$, $(2, 4, p)$.

In this paper we prove the following result, generalizing [1, Theorem 1.1].

THEOREM 1.1. *Let M be an odd squarefree positive integer,* $\gcd(M, 21) = 1$. *Then the equation*

$$x^n + y^n = 2^\alpha Mz^2 \tag{1.1}$$

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

Similarly, one can generalize the results from the paper by Bennett *et al.* [3] (see the remark in Section 3).

In Sections 4, 5 and 6 we give new proofs of results concerning solubility of specific diophantine equations of types $(3, 3, p)$ and $(4, 2, p)$. In these cases we reduce the problem to studying several diophantine equations of type $(p, p, 2)$.

2. Preliminaries

LEMMA 2.1. *Suppose that $p \geq 7$ is prime.*

(i) *If $(C, \alpha_0) \in \{(1, 2), (3, 2)\}$, then the equation $x^p + 2^\alpha y^p = Cz^2$ has no solutions in nonzero pairwise coprime integers (x, y, z) with $xy \neq \pm 1$ and integers $\alpha \geq \alpha_0$.*

(ii) *If $C \in \{1, 2\}$, then the equation $x^p + y^p = Cz^2$ has no solutions in nonzero coprime integers (x, y, z) with $xy \neq \pm 1$.*

PROOF. Special cases of Theorems 1.2 and 1.1 in [2]. See also [7, Main theorem]. □

LEMMA 2.2. *For non-zero integers x, y satisfying $\gcd(x, y) = 1$, we have:*

(i) $\gcd(x + y, x^2 + y^2) = 1$ *or* 2;

(ii) $\gcd(x + y, x^2 - xy + y^2) = 1$ *or* 3.

PROOF. (i) Assume $r^e | x + y$ and $r^e | x^2 + y^2$, where r is a prime and e is a positive integer. Then $r^e | 2x^2$. But $\gcd(x, y) = 1$, hence $r \nmid x$. Therefore $r^e | 2$ and the assertion follows. The proof of (ii) follows along the same lines. □

3. Generalization of Bennett and Mulholland's result

The proof of Theorem 1.1 follows along the same lines as the proof of [1, Theorem 1.1], therefore we only indicate the main steps. The genuine new ingredient is Lemma 3.1 below. The point is that a classification of elliptic curves over $\mathbb{Q}$ with rational 2-torsion point and conductor $32M^2$ or $256M^2$ is not necessary—here we use a much weaker result.

Let

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

denote the elliptic curve attached to nontrivial solution of (1.1). Let ρ_n^E denote the corresponding mod n Galois representation. Using [2, Lemmas 3.2 and 3.3] we obtain that this representation arises from a cuspidal newform of weight 2, trivial Nebentypus, and level $32M^2$ or $256M^2$. Let f be a cuspidal newform of weight 2, level N, and trivial Nebentypus, where $N = 32M^2$ or $256M^2$.

If f has at least one Fourier coefficient that is not a rational integer, then we obtain (analogously to [1]) $n \leq M^{12M^2}$ if $N = 32M^2$, and $n \leq M^{132M^2}$ if $N = 256M^2$.

If f has only rational integer Fourier coefficients, then we argue as in [1], replacing Propositions 3.1 and 3.2 by the following result.

LEMMA 3.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with rational 2-torsion and conductor $32M^2$ or $256M^2$, where M is an odd squarefree integer. If $\gcd(M, 21) = 1$, then E has j-invariant whose denominator is divisible by some prime $p_0 | M$ or CM by an order in $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$.*

PROOF. Write $M = p_1 \cdots p_k$. Generalizing [8, Lemme 1], we deduce that E has global minimal model of the form

$$y^2 = x(x^2 + ax + b),$$

with integers $a, b \in \mathbb{Z}$ without common prime factors different from $2, p_1, \ldots, p_k$. One can easily check that

$$c_4 = 2^4(a^2 - 3b), \quad c_6 = 2^5 a(9b - 2a^2), \quad \Delta_E = 2^4 b^2(a^2 - 4b).$$

If $a = 0$, then E has CM by $\mathbb{Q}(\sqrt{-1})$.

Assume that $a \neq 0$, and write

$$\Delta_E = \pm 2^m p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad a = \pm 2^{m_1} p_1^{\beta_1} \cdots p_k^{\beta_k} a_0, \quad b = \pm 2^{m_2} p_1^{\gamma_1} \cdots p_k^{\gamma_k}.$$

Using [12, Tableau IV] we obtain

$$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) \in \{(6, 4, \geq 6), (9, 4, 6), (12, 6, \geq 9), (12, 7, 9)\} \quad \text{if } N_E = 32M^2,$$

and

$$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) \in \{(9, 5, \geq 8), (15, 7, \geq 11)\} \quad \text{if } N_E = 256M^2.$$

If $2\beta_{i_0} < \gamma_{i_0}$ for some $i_0 \in \{1, \ldots, k\}$, then the denominator of j_E is divisible by p_{i_0}.

If $2\beta_i \geq \gamma_i$ for all $i \in \{1, \ldots, k\}$, then careful analysis of possible cases for $(v_2(\Delta_E), v_2(c_4), v_2(c_6))$ leads to elliptic curves with CM by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$, or to elliptic curves with j-invariants whose denominators are divisible by some prime $p_0 | M$. Let us give some details (possible values of (m_1, m_2) will follow from the formulas for c_4, c_6 and Δ_E, given above).

$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) = (6, 4, \geq 6)$. In this case $(m_1, m_2) = (0, 1)$ or $(>1, 0)$. If $(m_1, m_2) = (0, 1)$, then denominator of j_E is divisible by some $p_0 | M$, or $p_1^{2\beta_1 - \gamma_1} \cdots p_k^{2\beta_k - \gamma_k} a_0^2 \pm 8 = \pm 1$. In the second case $a_0 = \pm 3$ and $\gamma_i = 2\beta_i$ for all $i \in \{1, \ldots, k\}$ (here we use the assumption $\gcd(p_i, 21) = 1$), and we obtain a family of elliptic curves $y^2 = x^3 \pm 3Mx^2 + 2M^2 x$ with CM by $\mathbb{Q}(\sqrt{-1})$. The case $(m_1, m_2) = (>1, 0)$ leads to elliptic curves with j-invariants whose denominators are divisible by some $p_0 | M$.

$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) = (9, 4, 6)$. In this case $(m_1, m_2) = (1, 0)$, and we obtain elliptic curves with j-invariants whose denominators are divisible by some $p_0 | M$, or a family $y^2 = x^3 \pm 3Mx^2 + 2M^2 x$ with CM by $\mathbb{Q}(\sqrt{-1})$.

$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) = (9, 5, \geq 8)$. In this case $(m_1, m_2) = (\geq 2, 1)$, and we obtain elliptic curves with j-invariants whose denominators are divisible by some $p_0 | M$, or a family $y^2 = x^3 \pm 4Mx^2 + 2M^2 x$ with CM by $\mathbb{Q}(\sqrt{-2})$.

$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) = (12, 6, \geq 9)$. In this case $(m_1, m_2) = (1, 3)$, and we obtain elliptic curves with j-invariants whose denominators are divisible by some $p_0 | M$, or a family $y^2 = x^3 \pm 3Mx^2 + 2M^2 x$ with CM by $\mathbb{Q}(\sqrt{-1})$.

https://doi.org/10.1017/S000497271000033X Published online by Cambridge University Press

$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) = (12, 7, 9)$. This case produces no elliptic curve. Indeed, $m_1m_2 = 0$ implies $v_2(c_4) = 4$ or $v_2(\Delta_E) = 4$, a contradiction. Let $m_1m_2 \geq 1$. Then $m_1 = 1$ implies $m_2 = 2$, and hence $v_2(c_6) = 8$; similarly, $m_1 \geq 2$ implies $m_2 = 3$, and hence $v_2(c_6) \geq 10$.

$(v_2(\Delta_E), v_2(c_4), v_2(c_6)) = (15, 7, \geq 11)$. In this case $(m_1, m_2) = (\geq 3, 3)$, and we obtain elliptic curves with j-invariants whose denominators are divisible by some $p_0|M$, or a family $y^2 = x^3 \pm 8Mx^2 + 8M^2x$ with CM by $\mathbb{Q}(\sqrt{-2})$. □

REMARK 3.2. One can generalize [3, Theorems 1.1, 1.3 and 1.4]: here we replace Proposition 6.1 by a variant of Lemma 3.1. It is clear that variants of Lemma 3.1 will apply to some other types of generalized Fermat equations.

4. New proof of Billerey's result

Let p be an odd prime. Consider the equation

$$(x + y)(x^2 + y^2) = z^p, \quad \gcd(x, y) = 1. \tag{4.1}$$

By Lemma 2.2 we have two cases to consider.

(i) Assume that $\gcd(x + y, x^2 + y^2) = 2$. In this case $x + y = 2^{p-1}z_1^p$ and $x^2 + y^2 = 2z_2^p$, with $\gcd(z_1, z_2) = 1$. Substituting $y = -x + 2^{p-1}z_1^p$ in the second equation we obtain

$$2x^2 - 2^p z_1^p x + 2^{2p-2}z_1^{2p} - 2z_2^p = 0.$$

We have $\Delta_x = 16(z_2^p - 2^{2p-4}z_1^{2p})$. Using Lemma 2.1(i), we obtain that the equation $X^p + 2^mY^p = Z^2$ $(m \geq 2)$ has no solution in nonzero pairwise coprime integers (X, Y, Z) with $XY \neq 1$. As a corollary we obtain the following result [4, Theorem 3.1].

PROPOSITION 4.1. *Equation (4.1) has no nontrivial solution in integers x, y, z with z even.*

(ii) Assume that $\gcd(x + y, x^2 + y^2) = 1$. In this case $x + y = z_1^p$ and $x^2 + y^2 = z_2^p$, with $\gcd(z_1, z_2) = 1$. Substituting $y = -x + z_1^p$ in the second equation we obtain $2x^2 - 2z_1^p x + z_1^{2p} - z_2^p = 0$. We have $\Delta_x = 4(2z_2^p - z_1^{2p})$. It is expected that the equation $2X^p + Y^p = Z^2$, $\gcd(X, Y) = 1$, has no solutions in nonzero coprime integers (X, Y, Z) with $XY \neq \pm 1$, and hence (4.1) has no solutions. Such an expectation follows from [9, Conjecture 2], at least for p sufficiently large.

5. Application to the equation $x^3 + y^3 = z^p$

Let p be an odd prime. Consider the equation

$$x^3 + y^3 = z^p, \quad \gcd(x, y) = 1. \tag{5.1}$$

Assume that $p \geq 17$ and (a, b, c) is a nontrivial solution to Equation (5.1), satisfying ac even. Kraus [11, Theorem 6.1] has proved the following result.

PROPOSITION 5.1.

(i) *c is odd;*
(ii) $v_2(a) = 1$*;*
(iii) $v_3(c) \geq 1$.

We give another proof of this result. By Lemma 2.2 we have two cases to consider.

(i) Assume that $\gcd(x + y, x^2 - xy + y^2) = 1$. In this case $x + y = z_1^p$ and $x^2 - xy + y^2 = z_2^p$, with $\gcd(z_1, z_2) = 1$. Substituting $y = -x + z_1^p$ in the second equation, we obtain $3x^2 - 3z_1^p x + z_1^{2p} - z_2^p = 0$. We have $\Delta_x = 3(4z_2^p - z_1^{2p})$. Using Lemma 2.1(i), we obtain that the equation $4X^p + Y^p = 3Z^2$, $\gcd(X, Y) = 1$, has no nontrivial solution in integers satisfying $XY \neq \pm 1$. In particular, Equation (5.1) has no solution if z is even. This proves case (i).

(ii) Assume that $\gcd(x + y, x^2 - xy + y^2) = 3$. Then, in particular, $v_3(z) \geq 1$. In this case we have $x + y = 3^{p-1} z_1^p$ and $x^2 - xy + y^2 = 3z_2^p$, with $\gcd(z_1, z_2) = 1$. Substituting $y = -x + 3^{p-1} z_1^p$, we arrive at the diophantine equation $4z_2^p - 3^{2p-3} z_1^p = t^2$. Here we are in case (iii) from [2]: $A = 3^{p-3}$, $B = 4$, $C = 1$. Let $E = E_3(a, b, c)$ be the corresponding elliptic curve. Using [2, Lemma 3.3], we obtain that the corresponding Galois representation $\rho_{E,p}$ (with $p \geq 7$) arises from a cuspidal newform of weight 2 and level 12 (level 24) if $z_2 \equiv 3 \bmod 4$ ($z_2 \equiv 1 \bmod 4$). There are no nonzero cuspforms of weight 2 and level 12. In the case of level 24 we have $z_2 \equiv 1 \bmod 4$, hence $x \equiv 2 \bmod 4$, proving case (ii).

REMARKS 5.2.

(i) Note that $3^{p-3} \pm 4$ are not squares of integers. Therefore [9, Conjecture 1] implies that the equation $4X^p + 3^{p-3} Y^p = Z^2$ has no nontrivial solutions. Consequently (5.1) has no nontrivial solutions.
(ii) Kraus [11] showed that (5.1) has no nontrivial solutions for exponents p with $17 \leq p \leq 10^4$; the same can be proved for $5 \leq p \leq 13$.

6. Application to the equation $x^4 - y^2 = nz^p$

Let $p \geq 5$ be prime and n a positive integer greater than 1. Dąbrowski [6] proves that, under certain conditions on n, the equation $x^4 - y^4 = nz^p$ has no nontrivial solution in $\mathbb{Z}$ if $p \geq C(n)$, where $C(n)$ is effectively a constant. Let us state a particular case [6, Corollary 1].

PROPOSITION 6.1. *Let q be an odd prime, not of the type $2^m \pm 1$. Let p be a prime satisfying $p > (\sqrt{8q + 8} + 1)^{2q-2}$. Then the equation $x^4 - y^4 = qz^p$ has no nontrivial solution in the integers.*

We will deduce the following version of this result from [9]. We should stress that both proofs use ideas from [10].

PROPOSITION 6.2. *Let $q > 3$ be a prime; assume that $q \equiv 3 \bmod 8$ and $q \neq 2t^2 + 1$, or $q \equiv 5 \bmod 8$ and $q \neq t^2 + 4$. In addition, let p be a prime satisfying $p > (8\sqrt{q + 1} + 1)^{16(q-1)}$. Then the equation $x^4 - y^2 = qz^p$ has no nontrivial solution in the integers.*

https://doi.org/10.1017/S000497271000033X Published online by Cambridge University Press

PROOF. The case where xy is even leads to consideration of the diophantine equation $qX^p + Y^p = 2Z^2$. Theorem 1.2 in [9] implies that it has no nontrivial solution if $q \equiv 3 \bmod 8$ and $q \neq 2t^2 + 1$ or $q \equiv 5 \bmod 8$, and $p > (8\sqrt{q+1} + 1)^{16(q-1)}$.

The case where xy is odd leads to consideration of two diophantine equations:

(i) $X^p + 4qY^p = Z^2$;
(ii) $4X^p + qY^p = Z^2$.

Theorem 1.1 in [9] implies that these equations have no nontrivial solution if $q \equiv 3 \bmod 8$ or $q \equiv 5 \bmod 8$ and $q \neq t^2 + 4$, and $p > (8\sqrt{q+1} + 1)^{16(q-1)}$. □

REMARK 6.3. Some questions concerning solubility of a general diophantine equation $x^4 - y^2 = nz^p$ may be reduced to [9, Conjectures 1 and 2].

References

[1] M. A. Bennett and J. Mulholland, 'On the diophantine equation $x^n + y^n = 2^\alpha pz^2$', *C. R. Math. Acad. Sci. Soc. R. Can.* **28** (2006), 6–11.

[2] M. A. Bennett and C. M. Skinner, 'Ternary diophantine equations via Galois representations and modular forms', *Canad. J. Math.* **56** (2004), 23–54.

[3] M. A. Bennett, V. Vatsal and S. Yazdani, 'Ternary diophantine equations of signature $(p, p, 3)$', *Compositio Math.* **140** (2004), 1399–1416.

[4] N. Billerey, 'Formes homogènes de degré 3 et puissances p-ièmes', *J. Number Theory* **128** (2008), 1272–1294.

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

[6] A. Dąbrowski, 'On the integers represented by $x^4 - y^4$', *Bull. Aust. Math. Soc.* **76** (2007), 133–136.

[7] H. Darmon and L. Merel, 'Winding quotients and some variants of Fermat's last theorem', *J. reine angew. Math.* **490** (1997), 81–100.

[8] W. Ivorra, 'Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$', *Dissert. Math.* **429** (2004), 55pp.

[9] W. Ivorra and A. Kraus, 'Quelques résultats sur les équations $ax^p + by^p = cz^2$', *Canad. J. Math.* **58** (2006), 115–153.

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

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

[12] I. Papadopoulos, 'Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3', *J. Number Theory* **44** (1993), 119–152.

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

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

[15] A. Wiles, 'Modular elliptic curves and Fermat's last theorem', *Ann. of Math.* (2) **141** (1995), 443–551.

ANDRZEJ DĄBROWSKI, Institute of Mathematics, University of Szczecin,
ul. Wielkopolska 15, 70-451 Szczecin, Poland
e-mail: dabrowsk@wmf.univ.szczecin.pl

https://doi.org/10.1017/S000497271000033X Published online by Cambridge University Press