BULL. AUSTRAL. MATH. SOC. 11D41, 11F33, 11F80, 11G05
VOL. 76 (2007) [133–136]

ON THE INTEGERS REPRESENTED BY $x^4 - y^4$

ANDRZEJ DĄBROWSKI

Let p be a prime number $\geqslant 5$, and n a positive integer > 1. This note is concerned with the diophantine equation $x^4 - y^4 = nz^p$. We prove that, under certain conditions on n, this equation has no non-trivial solution in $\mathbf{Z}$ if $p \geqslant C(n)$, where $C(n)$ is an effective constant.

1. INTRODUCTION

By the work of Hellegouarch, Frey, Serre, Ribet, Wiles, Taylor and many others, we can reduce the study of a class of ternary diophantine equations (generalised Fermat equations) to modern techniques coming from Galois representations and modular forms. In all known cases, the proofs follow a variant of the method of Frey curves and Ribet's level-lowering theorem.

Let n be a positive integer > 1, and p an odd prime, $\gcd(n,p) = 1$. Let $v_l(n)$ be the exact power of l dividing n, and let $\alpha = v_2(n)$. Consider the equation

$$x^4 - y^4 = nz^p, \quad \gcd(x,y) = 1. \tag{1}$$

Let $N = 2^4 r'(n)$, where $r'(n)$ denotes the product of odd prime divisors of n. Let $g_0^+(N)$ denote the dimension of the $\mathbf{C}$-vector space of newforms of weight 2 with respect to the congruence subgroup $\Gamma_0(N)$. Let $\mu(N)$ be the index of $\Gamma_0(N)$ in $SL(2,\mathbf{Z})$. Put

$$F(N) := \left(\sqrt{\frac{\mu(N)}{6}} + 1\right)^{2g_0^+(N)}.$$

Darmon [1] showed that, for a prime number $p \geqslant 11$, the equation $x^4 - y^4 = z^p$ has no non-trivial solution if $p \equiv 1 (\bmod 4)$ or z is even. We combine the methods of Darmon [1] and Kraus [4] to prove the following general result.

Received 11th December, 2006
The article was written during my visit to the Max-Planck-Institut für Mathematik in Bonn in September-December 2006. I would like to thank the Institute for the hospitality and support.

Theorem 1.

(i) *Let $\alpha \geqslant 1$, and let p be a prime $\geqslant 5$. Then the equation*

$$x^4 - y^4 = 2^\alpha z^p, \quad \gcd(x, y) = 1 \tag{2}$$

has no non-trivial solution in integers.

(ii) *Let $\alpha \geqslant 1$ and let p be a prime $> \max\bigl(F(N), 3\bigr)$. Assume that $p \nmid n$ and $v_l(n) < p$ for any prime l. Assume that there is no elliptic curve over $\mathbf{Q}$ of conductor N, with all its 2-division points defined over $\mathbf{Q}$. Then (1) has no non-trivial solution in integers.*

(iii) *Let $\alpha = 0$ and let p be a prime $> \max\bigl(F(N), F(2N), 3\bigr)$. Assume that $p \nmid n$ and $v_l(n) < p$ for any prime l. Assume that there is no elliptic curve over $\mathbf{Q}$ of conductor N, with all its 2-division points defined over $\mathbf{Q}$. Then (1) has no non-trivial solution in integers.*

Let E be an elliptic curve over $\mathbf{Q}$, of conductor $2^k q$, q an odd prime. If E has all its 2-division points defined over $\mathbf{Q}$, then q is a Fermat or a Mersenne prime ([**3**], or [**4**, Lemma 6]). Using the arguments in ([**4**, p. 1162]), we obtain

Corollary 1. *Let q be an odd prime, not of the type $2^m \pm 1$, satisfying $p > \bigl(\sqrt{8q+8}+1\bigr)^{2q-2}$. Let $\alpha \geqslant 0$, $\beta > 0$ be integers. Then the equation $x^4 - y^4 = 2^\alpha q^\beta z^p$ has no non-trivial solution in integers.*

2. Proof of Theorem 1

Let $a^4 - b^4 = nc^p$ be a solution to equation (1). Let

$$E : y^2 = x^3 + 4abx^2 - (a^2 - b^2)^2 x \tag{3}$$

denote the corresponding Frey curve (compare [**1**]). We have

$$c_4 = 2^4\left[2^4a^2b^2 + 3(a^2 - b^2)^2\right], c_6 = -2^7\left[2^5a^2b^2 + 3^2(a^2 - b^2)^2\right],$$

and $\Delta = 2^6 n^2 (a^2 - b^2)^2 c^{2p}$. Let Δ_E and N_E denote the minimal discriminant and conductor of E, respectively.

Lemma 1.

(i) *If $\alpha = 0$ and c is odd, then $\Delta_E = 2^6 n^2 (a^2 - b^2)^2 c^{2p}$ and $N_E = 2^5 r'(nc)$.*

(ii) *If $\alpha \geqslant 1$ or c is even, then $\Delta_E = 2^{-6} n^2 (a^2 - b^2)^2 c^{2p}$ and $N_E = 2^4 r'(nc)$.*

Proof: (i) In this case a model (3) is global minimal. The curve has multiplicative reduction at any odd prime r dividing Δ_E, since $v_r(c_4) = 0$. On the other hand,

$v_2(c_4) = 4$, $v_2(c_6) = 7$ and $v_2(\Delta_E) = 6$, hence using [8], Table IV, we obtain $v_2(N) = 5$.
(ii) In this case, the model

$$y^2 = x^3 + abx^2 - 2^{-4}(a^2 - b^2)^2 x. \tag{4}$$

is global minimal. Here we have $v_2(c_4) = 4$, $v_2(c_6) = 6$ and $v_2(\Delta_E) \geqslant 12$, hence using again [8, Table IV], we obtain $v_2(N) = 4$. ∎

Let

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\big(E[p]\big) \simeq GL_2(\mathbf{F}_p)$$

be the Galois representation associated to the p-division points of E.

Lemma 2. *Assume $p \geqslant 5$. Then ρ is absolutely irreducible.*

Proof: E has all its 2-division points defined over $\mathbf{Q}$, hence the result follows from [6, Theorem 3] (If ρ is reducible, then we are in case (iii) with $p \leqslant 3$.); see also [7, Theorem 1.3]. ∎

Let $N(\rho)$ denote the Artin conductor of ρ, as defined in [10].

Lemma 3. *Let p be an odd prime,* $\gcd(n,p) = 1$. *We have $N(\rho) = 2^k r'(n)$, where $k = 5$ if $\alpha = 0$ or c is odd, and $k = 4$ if $\alpha \geqslant 1$ or c is even.*

Proof: E has additive reduction at 2, hence $v_2\big(N(\rho)\big) = v_2(N_E)$ (see [5]). Now use Lemma 1, and the properties of $N(\rho)$ ([10, p. 191]). ∎

Elliptic curves E defined by (3) are semistable at 3 and 5, hence modular due to the work of Wiles [11] and Diamond [2]. Applying the "lowering the level" result of Ribet [9] we conclude that ρ arises from a cuspidal newform of weight 2 and level $2^k r'(n)$.

Completion of the proof of Theorem 1. (i) The space of cuspidal newforms of weight 2 with respect to $\Gamma_0(16)$ is empty, hence the assertion follows. Proofs of (ii) and (iii) follow the same line as the proof of [4, Theorem 1]. We omit the details. ∎

References

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

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

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

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

[5] A. Kraus, 'Détermination du poids et du conducteur associé aux représentations des points de p-torsion d'une courbe elliptique', *Dissertationes Math.* **364** (1997), 39pp.

[6] B. Mazur, 'Rational isogenies of prime degree', *Invent. Math.* **44** (1978), 129–162.

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

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

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

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

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

Institute of Mathematics
University of Szczecin
ul. Wielkpolska 15
70-451 Szczecin
Poland
e-mail: dabrowski@sus.univ.szczecin.pl