COLLOQUIUM MATHEMATICUM

VOL. 123 2011 NO. 1

ON GENERALIZED FERMAT EQUATIONS OF SIGNATURE $(p,p,3)$

BY

KAROLINA KRAWCIÓW (Szczecin)

Abstract. This paper focuses on the Diophantine equation $x^n + p^\alpha y^n = Mz^3$, with fixed α, p, and M. We prove that, under certain conditions on M, this equation has no non-trivial integer solutions if $n \geq \mathcal{F}(M, p^\alpha)$, where $\mathcal{F}(M, p^\alpha)$ is an effective constant. This generalizes Theorem 1.4 of the paper by Bennett, Vatsal and Yazdani [Compos. Math. 140 (2004), 1399–1416].

1. Introduction. Fix non-zero integers A, B, and C. For given positive integers p, q, r satisfying $1/p+1/q+1/r < 1$, the generalized Fermat equation

$$Ax^p + By^q = Cz^r \tag{1.1}$$

has only finitely many proper integer solutions [5]. The proof uses the famous Theorem of Faltings [6] (Mordell conjecture). Modern techniques coming from Galois representations and modular forms (methods of Frey–Hellegouarch curves and variants of Ribet's level-lowering theorem) allow one to give partial (sometimes complete) results concerning the set of solutions to (1.1), at least when (p,q,r) is of the type (p,p,p), $(p,p,2)$, $(p,p,3)$, $(4,4,p)$, $(3,3,p)$, $(5,5,p)$ or $(2,4,p)$. For the first four signatures, the results are mostly of the type: *there is no primitive integer solution in x, y, z if p is larger than some positive constant depending on A, B, and C* (see, for instance, [7], [1], [4], [2], [3]).

In this article we generalize Theorem 1.4 from [2]. Such a possibility was pointed out by A. Dąbrowski (see [4, Remark to Lemma 3]).

Consider the Diophantine equation

$$x^n + p^\alpha y^n = Mz^3, \tag{1.2}$$

where n and p are prime numbers, M is a non-zero integer, and α is a non-negative integer. We prove, under some assumptions on M and p, the existence of a positive constant $\mathcal{F}(M, p^\alpha)$ such that for all primes $n > \mathcal{F}(M, p^\alpha)$ the equation (1.2) has no solutions in non-zero coprime integers x, y and z. More precisely, we prove the following results. Let $\tilde{M}$ denote the radical of M (the product of all prime divisors of M).

2010 *Mathematics Subject Classification*: Primary 11D41.

Key words and phrases: Diophantine equation, elliptic curve.

DOI: 10.4064/cm123-1-4

THEOREM 1.1. *Let n be a prime number, and let M be a non-zero cube-free integer, divisible by 3. If $n > \tilde{M}^{10\tilde{M}^2}$, then the Diophantine equation*

$$x^n + y^n = Mz^3$$

has no non-trivial solutions in coprime integers x, y and z.

Fix odd primes $p_1, \ldots, p_k$; assume $3 \in \{p_1, \ldots, p_k\}$. Theorem 1.1 implies that the 2^{k+1} Diophantine equations

$$x^\alpha - p_1^{\alpha_1} \ldots p_k^{\alpha_k} y^3 = \pm 1 \quad (1 \le \alpha_i \le 2,\ i = 1, \ldots, k)$$

have only finitely many solutions in integers $y > 1$, $\alpha > 1$, and primes x. Let $P(p_1, \ldots, p_k)$ denote the finite set of primes x satisfying any of the above 2^{k+1} Diophantine equations. It should be clear that it is not easy to determine the set $P(p_1, \ldots, p_k)$. It can be checked (and is implicitly contained in [2]) that $P(3) = \{2, 5\}$. Variants of Theorem 1.5 in [2] (plus some additional work) should give, in principle, an exact description of $P(3, q)$ for small primes q.

THEOREM 1.2. *Let $M = \prod_{i=1}^k p_i^{\gamma_i}$ be a positive cube-free integer, divisible by 3, α a positive integer, and n a prime. If p is a prime such that $p \notin P(p_1, \ldots, p_k)$ and $p \neq \prod_{i=1}^k p_i^{\alpha_i} s^3 \pm 1$ $(1 \le \alpha_i \le 2,\ i = 1, \ldots, k)$ for any integer s, and if $n > (p\tilde{M})^{10p\tilde{M}^2}$, then the Diophantine equation*

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

has no non-trivial solutions in coprime integers x, y, and z.

This result generalizes Theorem 1.4 from [2], where the authors considered $M = 3^\beta$.

2. Proofs of Theorems 1.1 and 1.2. The proofs of Theorems 1.1 and 1.2 follow the same lines as the proofs of Theorems 1.1, 1.3 and 1.4 in [2], hence we only indicate the main steps. The new ingredients are Lemmas 2.1 and 2.2 below (they correspond to Proposition 6.1 in [2]).

Let us suppose that $n \ge 11$ and p are prime numbers, let $\alpha \ge 0$ be an integer smaller than n, and let M be a non-zero, cube-free integer, divisible by 3. As in [2], we associate to the primitive solution (a, b, c) of (1.2) the elliptic curve

$$E = E(a, b, c) : y^2 + 3Mcxy + M^2 p^\alpha b^n y = x^3.$$

Let

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

denote the corresponding mod n Galois representation on the n-torsion $E[n]$ of E. Write $M = 3^\gamma \prod p_i^{\gamma_i}$. Via Lemma 3.4 of [2], this representation arises from a cuspidal newform f of weight 2, trivial Nebentypus character, and level $N = 3^5 \prod p_i^2$ (if $\alpha = 0$) or $N = 3^5 p \prod p_i^2$ (if $\alpha > 0$).

If f has at least one non-rational Fourier coefficient, then (applying Theorem 2 in [8], and arguing as in [2, Section 7]) we obtain $n \le \tilde{M}^{10\tilde{M}^2}$ (if $\alpha = 0$) or $n \le (p\tilde{M})^{10p\tilde{M}^2}$ (if $\alpha > 0$).

If f has only rational Fourier coefficients, then it corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor N. Now we argue as in [2], replacing Proposition 6.1 there by the following results.

LEMMA 2.1. *Let F be an elliptic curve defined over $\mathbb{Q}$ with a rational 3-torsion point and conductor $3^5 \prod_{i=2}^k p_i^2$. Then F has complex multiplication by an order in $\mathbb{Q}(\sqrt{-3})$.*

LEMMA 2.2. *If p and $p_2, \dots, p_k$ are primes such that $p \notin P(3, p_2, \dots, p_k)$, and $p \ne 3^{\alpha_1} \prod_{i=2}^k p_i^{\alpha_i} s^3 \pm 1$ ($1 \le \alpha_i \le 2$, $i = 1, \dots, k$) for any integer s, then there is no elliptic curve defined over $\mathbb{Q}$ with a rational 3-torsion point and conductor $3^5 p \prod_{i=2}^k p_i^2$.*

Proofs of Lemmas 2.1 and 2.2. Any elliptic curve defined over $\mathbb{Q}$ with a rational 3-torsion point is isomorphic to a curve given by the Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3,$$

where a_1 and a_3 are integers; we may assume $a_3 > 0$. We may (and will) further assume that if a prime q divides a_1, then q^3 does not divide a_3, so the equation is minimal at q. One easily checks that

$$c_4 = a_1(a_1^3 - 24a_3), \quad c_6 = -a_1^6 + 36a_1^3 a_3 - 216a_3^2, \quad \Delta_F = a_3^3(a_1^3 - 27a_3).$$

The conductor N_F of the curve F equals $3^5 p^\epsilon \prod_{i=2}^k p_i^2$, where $\epsilon \in \{0, 1\}$. We rewrite

$$a_1 = \pm 3^\alpha p^{\alpha_0} \prod_{i=2}^k p_i^{\alpha_i} a, \quad a_3 = 3^\beta p^{\beta_0} \prod_{i=2}^k p_i^{\beta_i}, \quad \Delta_F = \pm 3^\delta p^{\delta_0} \prod_{i=2}^k p_i^{\delta_i}.$$

Using [9, Tableau II], we obtain

$$(v_3(c_4), v_3(c_6), v_3(\Delta_F)) \in \{(\ge 3, 4, 5), (\ge 4, 5, 7), (\ge 5, 7, 11), (\ge 6, 8, 13)\}.$$

Comparing this with the definitions of c_4, c_6 and Δ_F (given above), we deduce that the only possible values of (α, β, δ) are $(\ge 2, 1, 7)$ and $(\ge 2, 2, 11)$.

The elliptic curve F has bad additive reduction at 3 and at all primes p_i, $i = 2, \dots, k$, hence $3 \prod p_i$ divides both Δ_E and c_4. This implies that $3 \prod p_i$ divides a_1 and a_3 as well.

Suppose that $\epsilon = 0$. Then the integer

$$D = \frac{a_1^3}{27a_3} - 1 = \pm 3^{3\alpha - 3 - \beta} \prod_{i=2}^k p_i^{3\alpha_i - \beta_i} a^3 - 1$$

divides Δ_F. On the other hand it is coprime to Δ_F, so $D = -1$ and $a_1 = 0$. Therefore the curve F has j-invariant equal to 0, and hence has complex multiplication by an order in $\mathbb{Q}(\sqrt{-3})$.

Suppose $\epsilon = 1$. In this case F has bad multiplicative reduction at p. It is clear that p does not divide a_1, and either $p \mid a_3$ or $p \mid (a_1^3 - 27a_3)$. In both cases we obtain

$$p^r \pm 1 = 3^{3\alpha-3-\beta} \prod_{i=2}^{k} p_i^{3\alpha_i-\beta_i} a^3.$$

This completes the proofs of Lemmas 2.1 and 2.2. ∎

It is obvious that Lemma 2.2 implies Theorem 1.2. To prove Theorem 1.1 we apply Proposition 4.3 from [2].

Acknowledgements. The author would like to thank Prof. Andrzej Dąbrowski for inspiring suggestions and improvements to the preliminary version of this paper.

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, V. Vatsal and S. Yazdani, *Ternary diophantine equations of signature* $(p, p, 3)$, Compos. Math. 140 (2004), 1399–1416.
[3] A. Dąbrowski, *On the integers represented by* $x^4 - y^4$, Bull. Austral. Math. Soc. 76 (2007), 133–136.
[4] —, *On a class of generalized Fermat equations*, ibid. 82 (2010), 505–510.
[5] 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.
[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366; Erratum: 75 (1984), 381.
[7] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. 49 (1997), 1139–1161.
[8] G. Martin, *Dimensions of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, J. Number Theory 112 (2005), 298–331.
[9] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3*, J. Number Theory 44 (1993), 119–152.

Karolina Krawciów
Institute of Mathematics
University of Szczecin
70-451 Szczecin, Poland
E-mail: karolina.krawciow@wmf.univ.szczecin.pl

Received 9 March 2010;
revised 13 November 2010 (5345)