Journal de Théorie des Nombres
de Bordeaux **18** (2006), 315–321

The equation $x^{2n} + y^{2n} = z^5$

par Michael A. BENNETT

Résumé. Nous montrons que l'équation diophantienne ci-dessus n'admet pas de solutions entières x, y, z, telles que $(x, y) = (y, z) = (x, z) = 1$ et $xyz \neq 0$. La démonstration utilise les courbes de Frey et des résultats liés à la modularité des représentations galoisiennes.

Abstract. We show that the Diophantine equation of the title has, for $n > 1$, no solution in coprime nonzero integers x, y and z. Our proof relies upon Frey curves and related results on the modularity of Galois representations.

1. Introduction

Diophantine equations of the shape

$$x^p + y^q = z^r \tag{1.1}$$

have received a great deal of attention, both classically and more recently, spurred on by the spectacular proof of Fermat's Last Theorem by Wiles [15]. If we restrict our attention to positive integers p, q and r with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 \tag{1.2}$$

and insist upon the additional (and, as it transpires, necessary) hypothesis that x, y and z are nonzero and coprime, then a theorem of Darmon and Granville [6] ensures that, for a fixed triple (p, q, r), we encounter at most finitely many such solutions (x, y, z) to (1.1). Indeed, a folklore conjecture (and consequence of the ABC-conjecture of Masser and Oesterlé) is that (1.1) has only finitely many "nontrivial" solutions, not just for p, q and r fixed, but even if we allow them to vary, subject to (1.2) (provided one counts solutions corresponding to the identity $2^3 + 1^n = 3^2$ only once). If one were ambitious, one might even go so far as to specify a hopefully complete list of solutions (see e.g [11] and its Math Review by Bremner (98j:11020) for some historical perspectives on this conjecture and a partial cast of characters to whom it might arguably be attributed).

Manuscrit reçu le 8 octobre 2004.

Recent work on equations of type (1.1) under condition (1.2) have mostly followed the trail blazed by Wiles. For surveys of this emerging field, the reader is directed to papers of Kraus [10] and Merel [12], or, for more recent developments, to, e.g. [2] and [8]. While many partial results are available, the only infinite families (p, q, r) for which we know equation (1.1) to have no nontrivial solutions are those with $p = q$ and $r \in \{2, 3, p\}$ ([7], [15]) and those of the form $(p, q, r) = (2, 4, r)$ (see [8]) and $(p, q, r) = (2, q, 4)$ or $(4, q, 2)$ (under thin disguise, these may be found in [2]). For the case $p = q$ and arbitrary fixed r, Darmon [5] outlines a program to treat equation (1.1), via an ambitious generalization of the Frey-Ribet-Wiles approach. To carry out this program, one requires analogues of fundamental results of Mazur, Ribet and Wiles concerning elliptic curves and their associated Galois representations, for the case of representations attached to Jacobians of higher genus curves. The absence of such results ensures that, for example, we cannot currently establish the aforementioned conjecture for equations of the shape

$$x^n + y^n = z^5. \tag{1.3}$$

In this short note, our goal is to demonstrate that, while (1.3) may be presently unattainable, if we add the additional constraint that n is even, we obtain another infinite family of (p, q, r) for which equation (1.1) possesses only trivial solutions. To be precise, we prove

Theorem 1.1. *If $n \geq 2$ is an integer, then the Diophantine equation*

$$x^{2n} + y^{2n} = z^5 \tag{1.4}$$

has no solutions in coprime nonzero integers x, y and z.

There are, of course, many solutions to (1.4) if we drop the restriction of coprimality, e.g. $x = y = z = n = 2$. It is worth noting that our argument is essentially limited to (1.1) with $(p, q, r) = (2n, 2n, 5)$. Even the similar equation

$$x^{2n} - y^{2n} = z^5$$

is apparently beyond our grasp. Additionally, for the cases $(p, q, r) = (n, n, 2)$ or $(n, n, 3)$, unlike for $(n, n, 5)$, it seems that treating the equations

$$x^n + y^n = z^2 \quad \text{or} \quad x^n + y^n = z^3$$

for even values of n is not appreciably easier than dealing with the case of arbitrary n (though, as an historical aside, the first of these equations was known by Lebesgue, as early as 1840, to have no nontrivial solutions with $n = 2k$, provided a like conclusion holds for the Fermat equation $x^k + y^k = z^k$).

As a final comment, we should note that a like result to Theorem 1.1 was claimed by Battaglia [1]. It appears, however, that the arguments of

[1] are applicable only in a rather restricted setting; the reader is directed to the corresponding Mathematical Review of Swift [11D48-69].

2. Preliminaries

We begin with an easy, classical lemma; we include its proof for the sake of completeness.

Lemma 2.1. *If, for coprime nonzero integers* a, b *and* c*, we have*

$$a^2 + b^2 = c^5$$

then necessarily there exist coprime nonzero integers u *and* v*, of opposite parity, for which*

$$a = u\left(u^4 - 10u^2v^2 + 5v^4\right)$$

and

$$b = v\left(v^4 - 10u^2v^2 + 5u^4\right).$$

Proof. Since integral squares are congruent to $0, 1$ or 4 modulo 8, it follows, assuming $\gcd(a, b) = 1$, that a and b are of opposite parity. Thus factoring implies that

$$a + ib = (u + iv)^5$$

for some (coprime) integers u and v. Expanding this and equating real and imaginary parts leads to the stated expressions for a and b. The fact that a and b are of opposite parity, together with the coprimality of u and v, leads to the conclusion that u and v are also of opposite parity. □

Here and henceforth, we will assume (without loss of generality) that $n \geq 2$ is prime. From Lemma 2.1, if we have a solution to equation (1.4) in, say, positive, coprime integers x, y and z, we may suppose that

$$x^n = u\left(u^4 - 10u^2v^2 + 5v^4\right) \tag{2.1}$$

and

$$y^n = v\left(v^4 - 10u^2v^2 + 5u^4\right) \tag{2.2}$$

for coprime integers u and v of opposite parity. Since u and v are coprime, it follows that

$$\gcd\left(u, u^4 - 10u^2v^2 + 5v^4\right) = \gcd(u, 5) \in \{1, 5\}$$

and similarly

$$\gcd\left(v, v^4 - 10u^2v^2 + 5u^4\right) = \gcd(v, 5) \in \{1, 5\}.$$

We treat the cases $n \geq 7$ and $n \in \{2, 3, 5\}$ separately. In the former situation, we will appeal to connections between Frey curves and modular

forms. While we could, in fact, shorten our exposition by direct citation of results from [2] (e.g. Theorems 1.2 and 1.5), we will include a reasonable amount of detail, in the interests of keeping the paper at hand somewhat self-contained.

3. The cases $n \geq 7$

Let us begin by assuming that $n \geq 7$ and that $\gcd(uv, 5) = 1$. It follows from (2.1) and (2.2) that there exist coprime integers A, B, C and D such that

$$u = A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B^n \tag{3.1}$$

and

$$v = C^n \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = D^n, \tag{3.2}$$

where, without loss of generality, u and hence A is even. Combining (3.1) and (3.2), we have that

$$D^n + 20A^{4n} = w^2$$

where we write $w = v^2 - 5u^2$.

Following [6] (where we have made minor modifications to ensure our model's minimality at the prime 2; see [2]), define a (Frey) elliptic curve E via

$$E \ : \ Y^2 + XY = X^3 + \frac{(w-1)}{4}X^2 + \frac{5A^{4n}}{16}X.$$

To E we associate a Galois representation

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

on the n-torsion points $E[n]$ of E. Since $n \geq 7$, one can show that this representation is necessarily absolutely irreducible and hence, via work of Wiles [15] and Ribet [13] (see Lemma 3.3 of [2] for details), arises from a weight 2 cuspidal newform of trivial character and level 10, contradicting the fact that no forms of such a low level exist. The key fact here is the parity of A, which ensures (since n is not too small) that E has multiplicative reduction at 2 (and hence that the level of the corresponding newform is not divisible by 4).

Next, let us suppose that $\gcd(uv, 5) = 5$, say, $5 \mid u$. It follows that there exist coprime integers A, B, C and D such that we have both (3.2) and

$$u = 5^{n-1}A^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5B^n. \tag{3.3}$$

Combining (3.2) with (3.3), we thus have

$$B^n + 4\,C^{4n} = 5w_1^2 \tag{3.4}$$

and

$$D^n + 4 \cdot 5^{4n-3}A^{4n} = w_2^2, \tag{3.5}$$

where

$$w_1 = u^2/5 - v^2 \quad \text{and} \quad w_2 = v^2 - 5u^2.$$

Again, one of A or C is even. In the first case, we consider

$$E_1 \ : \ Y^2 + XY = X^3 + \frac{(w_2 - 1)}{4}X^2 + \frac{5^{4n-3}A^{4n}}{16}X$$

and, in the second,

$$E_2 \ : \ Y^2 + XY = X^3 + \frac{(5w_1 - 1)}{4}X^2 + \frac{5\,C^{4n}}{16}X.$$

As previously, from Lemma 3.3 of [2], we may conclude that E_1 corresponds to a weight 2, level 10 cuspidal newform and hence reach a contradiction. On the other hand, the curve E_2 (more precisely, the corresponding Galois representation on the n-torsion of E_2) gives rise to a weight 2 cuspidal newform

$$f = f_E = \sum_{n=1}^{\infty} c_n q^n$$

of trivial character and level 50 (the space of such forms has dimension 2 over $\mathbb{C}$). For this form and a prime $p \notin \{2, 5, n\}$, we have

$$\operatorname{trace} \rho_n^E(\mathrm{Frob}_p) \equiv c_p \mod n$$

where (see Lemma 4.2 of [2])

$$\operatorname{trace} \rho_n^E(\mathrm{Frob}_p) = \begin{cases} \pm(1+p) & \text{if } p \text{ divides } BC \\ 2\,t & \text{if } p \text{ fails to divide } BC. \end{cases}$$

Here, t is an integer satisfying $|t| \leq \sqrt{p}$. In particular, considering the case $p = 3$ and noting that, for each cuspidal newform f at level 50, we have $c_3 = \pm 1$ (see e.g. [14]), we deduce a contradiction from the assumption that $n \geq 7$.

4. The cases $n \in \{2, 3, 5\}$

In case $n = 5$, our theorem is a direct consequence of Fermat's Last Theorem [15] (or, more precisely, the special case of it first proved by Dirichlet in 1825). If $n = 3$, we may invoke a comparatively recent result of Bruin [3], who treated the more general equation

$$x^3 + y^3 = z^5$$

via Chabauty-style techniques (and showed that it has no solutions in coprime nonzero integers).

Let us therefore suppose that $n = 2$. From (2.1) and (2.2), if uv is coprime to 5, there exist integers A and B for which

$$u^4 - 10u^2v^2 + 5v^4 = \pm A^2 \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm B^2,$$

at least one of which is a contradiction modulo 8. We may thus assume, without loss of generality, that $5 \mid u$. Working modulo 8, from (2.1) and (2.2) we infer that u is even and v odd, and hence the existence of a positive integer A for which

$$A^2 = v^4 - 10u^2v^2 + 5u^4. \tag{4.1}$$

Here, as previously, u and v are nonzero. Writing

$$Y = \frac{4v\left(A + v^2 - 5u^2\right)}{u^3} \text{ and } X = \frac{2\left(A + v^2 - 5u^2\right)}{u^2},$$

we find that the curve defined by (4.1) is birational to the elliptic curve

$$F \,:\, Y^2 = X^3 + 20X^2 + 80X,$$

given as 400D1 in Cremona's tables [4]. Via 2-descent, it is easy to show that

$$F\left(\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z}$$

with the only rational points being at infinity and the 2-torsion point $(X, Y) = (0, 0)$. Since both of these correspond to $u = 0$ on our original curve (4.1), we obtain a contradiction. This completes the proof of Theorem 1.1.

5. Acknowledgments

I would like to thank Imin Chen for a number of stimulating discussions on these and related themes.

References

[1] A. Battaglia, *Impossibilità dell'equazione indeterminata* $x^{2n} + y^{2n} = z^5$. Archimede **20** (1968), 300–305.

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

[3] N. Bruin, *On powers as sums of two cubes*. Algorithmic number theory (Leiden, 2000), 169–184, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[4] J. Cremona, *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1992.

[5] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*. Duke. Math. J. **102** (2000), 413–449.

[6] H. Darmon, 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.

[7] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*. J. Reine Angew Math. **490** (1997), 81–100.

[8] J. S. 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.

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

[10] A. Kraus, *On the equation* $x^p + y^q = z^r$*: a survey*. Ramanujan J. **3** (1999), 315–333.

[11] R.D. Mauldin, *A generalization of Fermat's last theorem: the Beal conjecture and prize problem*. Notices Amer. Math. Soc. **44** (1997), 1436–1437.

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

[13] K. Ribet, *On modular representations of Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*. Invent. Math. **100** (1990), 431–476.
[14] W. Stein, *Modular forms database*. http://modular.fas.harvard.edu/Tables/
[15] A. Wiles, *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) **141** (1995), 443–551.

Michael A. Bennett
University of British Columbia
1984 Mathematics Road
Vancouver, B.C. Canada
E-mail : bennett@math.ubc.ca
URL: http://www.math.ubc.ca/ bennett/