Journal de Théorie des Nombres
de Bordeaux **15** (2003), 839–846

On the diophantine equation $x^2 = y^p + 2^k z^p$

par Samir SIKSEK

Résumé. Nous étudions l'équation du titre en utilisant une courbe de Frey, le théorème de descente du niveau de Ribet et une méthode due à Darmon et Merel. Nous pouvons déterminer toutes les solutions entières x, y, z, premières deux à deux, si $p \geq 7$ est premier et $k \geq 2$. De cela, nous déduisons des résultats sur quelques cas de cette équation qui ont été étudiés dans la littérature. En particulier, nous pouvons combiner notre résultat avec les résultats précédents de Arif et Abu Muriefah, et avec ceux de Cohn pour obtenir toutes les solutions de l'équation $x^2 + 2^k = y^n$ pour $n \geq 3$.

Abstract. We attack the equation of the title using a Frey curve, Ribet's level-lowering theorem and a method due to Darmon and Merel. We are able to determine all the solutions in pairwise coprime integers x, y, z if $p \geq 7$ is prime and $k \geq 2$. From this we deduce some results about special cases of this equation that have been studied in the literature. In particular, we are able to combine our result with previous results of Arif and Abu Muriefah, and those of Cohn to obtain a complete solution for the equation $x^2 + 2^k = y^n$ for $n \geq 3$.

1. Introduction

In [8] Darmon and Merel study the diophantine equation $x^2 = y^p + z^p$ along with two other variants of Fermat's equation. In this paper we show that the method of Darmon and Merel can be adapted to give results about the more general equation

$$x^2 = y^p + 2^k z^p \tag{1}$$

where k is a positive integer, and p a prime. Studying this equation unifies the study of two well-known exponential diophantine equations appearing in the literature: $x^2 + 2^k = y^n$ and $x^2 - 2^k = y^n$ (see [1], [3], [5], [6], [10]). We shall call an integral solution x, y, z of equation (1) primitive if x, y, z are pairwise coprime, and non-trivial if $xyz \neq 0$. The reader is forewarned

Manuscrit reçu le 24 juin 2002.
This work is funded by a grant from Sultan Qaboos University, Oman (IG/SCI/DOMS/02/06).

that our definitions of non-trivial and primitive are different from those of [8]. Our main result is the following.

Theorem 1. *Suppose $k \geq 2$ and that $p \geq 7$ is prime. Then the only non-trivial primitive solutions of equation (1) are $k = 3, x = \pm 3, y = z = 1$ and p arbitrary.*

In Section 3 we will give the implications of this theorem to the two aforementioned exponential equations. In particular, we are able to combine our theorem with earlier results of Arif and Abu Muriefah, and of J.H.E. Cohn, to give a complete solution to the equation $x^2 + 2^k = y^n$.

Our approach in proving Theorem 1 is to associate to each putative solution of equation (1) a Frey curve and apply Ribet's level-lowering theorem to show that the Galois representation on the p-torsion is isomorphic to a representation of a much smaller level. This will be sufficient to eliminate all the cases of the theorem except for $k = 3$ where we have to (slightly) adapt the method of Darmon and Merel. Since we are following well-trodden paths here, our exposition will be rather terse. Apart from [8] the reader may wish to compare what follows with [7] and [12, pages 397–399].

It has recently come to my attention that W. Ivorra [11] proves stronger results for equations (1) and (7) using similar methods.

2. Proof of Theorem 1

Assume the existence of a non-trivial primitive solution with $k \geq 2$ and $p \geq 7$ prime. We will show that this forces $k = 3$ and $y = z = 1$. It is helpful to give a complete list of assumptions we make about x, y, z, k, p

(1) Equation (1) is satisfied.
(2) $k \geq 2$.
(3) $p \geq 7$ is prime.
(4) x, y, z are pairwise coprime, odd, and non-zero.
(5) $x \equiv 3 \pmod 4$.

There is no loss of generality in making these assumptions; for the fourth statement above we need to absorb any power of 2 dividing z into the 2^k in equation (1). For the fifth one we need to replace x by $-x$ if necessary.

2.1. The Frey Curve. Denote by E the 'Frey curve'

$$E : Y^2 = X(X^2 + 2xX + y^p). \tag{2}$$

In standard notation we have,

$$c_4 = 16(4x^2 - 3y^p), \qquad \Delta = 2^{k+6}(y^2 z)^p, \qquad j = \frac{(4x^2 - 3y^p)^3}{2^{k-6}(y^2 z)^p}\ .$$

Let $\Delta_{\min}$ be the minimal discriminant of E, and N be its conductor. Finally, if α is a non-zero integer then denote by $\operatorname{rad}(\alpha)$ the product of distinct primes dividing α.

Lemma 1. *The values of $\Delta_{\min}$ and N are given by the following table:*

	$\Delta_{\min}$	N
$k=2$	$2^8(y^2z)^p$	$2^2\mathrm{rad}(yz)$ *or* $2^4\mathrm{rad}(yz)$
$k=3$	$2^9(y^2z)^p$	$2^5\mathrm{rad}(yz)$
$k=4$	$2^{10}(y^2z)^p$	$2^3\mathrm{rad}(yz)$
$k=5$	$2^{11}(y^2z)^p$	$2^3\mathrm{rad}(yz)$
$k=6$	$(y^2z)^p$	$\mathrm{rad}(yz)$
$k>6$	$2^{k-6}(y^2z)^p$	$2\mathrm{rad}(yz)$

Proof. It is easy to show that c_4 and Δ are not simultaneously divisible by any odd prime. We deduce thus that the curve is minimal and has multiplicative reduction at all primes dividing yz and at no other odd primes. This shows that the table entries are correct modulo powers of 2. It remains to study the reduction at 2. Recall that $x^2 = y^p + 2^k z^p$. Thus we may rewrite the equation for E as

$$Y^2 = X(X+x)^2 - 2^k z^p X. \tag{3}$$

Suppose first that $k \geq 6$. Replace X by $4X - x$ and Y by $8Y + 4X$. After simplifying we reach the model

$$Y^2 + XY = X^3 - \frac{(x+1)}{4}X^2 - 2^{k-4}z^p X + 2^{k-6}z^p x. \tag{4}$$

This model is integral since we assumed that $x \equiv 3 \pmod 4$. It is minimal at 2 since the 'new c_4' is $4x^2 - 3y^p$ which is odd. Hence this model is global minimal. The formulas for $\Delta_{\min}$ for the cases $k=6$ and $k>6$ are now immediate on noting that the change of variable above forces $\Delta_{\min} = 2^{-12}\Delta$.

If $k=6$ then clearly 2 does not divide $\Delta_{\min}$ and so it does not divide N. Thus suppose $k \geq 7$. The reduction modulo 2 of the model (4) is

$$Y^2 + XY = \begin{cases} X^3 & \text{or,} \\ X^3 + X^2. \end{cases}$$

In either case the singularity at $(0,0)$ is a node. This shows that 2 divides the conductor N precisely once.

For $k = 2,3,4,5$, it is clear that the curve is already minimal at 2 since 2^{12} does not divide Δ. The rest now follows from Tate's algorithm. For the benefit of the reader who would like to verify the details we point out that it is best to make the following changes of variable in the model (3) at the outset:

- If $k=5$ replace X by $X-x$ and Y by $Y+X$.
- If $k=4$ replace X by $X-x$ and Y by $Y+X+4$.
- If $k=3$ replace X by $X-x$ and Y by $Y+X$.
- If $k=2$ replace X by $X-x$ and Y by $Y+X+2$.

□

2.2. The Galois Representation. Now let

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

be the Galois representation on the p-torsion of E. To be able to apply Ribet's level-lowering theorem, and complete our proof, we will need to show that ρ is irreducible. For this we need two lemmas, the first of which is elementary.

Lemma 2. *The equation $a^2 = \pm 1 \pm 2^m$ has no solutions for $m \geq 2$ except for $3^2 = 1 + 2^3$.*

Lemma 3. *The j-invariant of E is non-integral except if $k = 3$ and $y = z = 1$.*

Proof. Suppose that the j-invariant

$$j = \frac{(4x^2 - 3y^p)^3}{2^{k-6}(y^2 z)^p}$$

is integral. It is easy to use this and the assumptions listed at the outset of the proof about x, y, z, k, p to show that $y = \pm 1$ and $z = \pm 1$. From equation (1) we see that $x^2 = \pm 1 \pm 2^k$, and this forces $k = 3$ and $y = z = 1$ by the previous Lemma. □

Lemma 4. *ρ is irreducible.*

Proof. If we are in the case $k = 3$ and $y = z = 1$ then the curve E is curve 32A4 in Cremona's tables [4] and so we know that it does not have isogenies of odd degree. Thus ρ is irreducible. Suppose we are not in this case. We note the following,

- E has a point of order 2. This is clear from the model (2) given for E.
- The j-invariant of E is non-integral (by the previous lemma).
- E has some odd prime of multiplicative reduction. Otherwise, from the formulas for the conductor given in Lemma 1 we see that $y = \pm 1$ and $z = \pm 1$, which is impossible as above.

These three properties are enough to force the irreducibility of ρ for $p \geq 7$; for this see the proof of [8, Theorem 7]. □

2.3. Conclusion of the Proof. It has been shown that all elliptic curves over $\mathbb{Q}$ are modular [2]. However, we note in passing that our Frey curve E has semistable reduction away from 3 and 5 (by Lemma 1), and so its modularity follows from an earlier theorem of Diamond [9] which is a strengthening of the work of Wiles and Taylor [18],[17].

Let $N(\rho)$ be the Serre conductor of ρ (see [15, page 180] for the definition). It follows from the properties of the Serre conductor and our Lemma 1 that

- $N(\rho) | 2^4$ if $k \neq 3$,
- $N(\rho) = 2^5$ if $k = 3$.

For this see [15, page 207] or [7, page 264]. Applying Ribet's level-lowering theorem [14] we see that ρ corresponds to a mod p eigenform of weight 2 and level $2, 4, 8$ or 16 if $k \neq 3$ and of level 32 if $k = 3$. Since there are no weight 2 cusp forms of levels $2, 4, 8, 16$ we immediately deduce that $k = 3$.

We will henceforth assume that $k = 3$, and to complete our proof we must show that $y = z = 1$. The rest of our proof will mimic the approach made by Darmon and Merel [8, pages 88–99] for the equation $x^p + y^p = z^2$ (which really corresponds to the case $k = 0$ of our equation 1). We saw above that ρ corresponds to a mod p eigenform of weight 2 and level 32, and we know that our Frey curve E possesses a point of order 2. This is exactly the same situation as in Darmon-Merel for their equation mentioned above. Their arguments show that if $p \equiv 1 \pmod 4$ then E has potentially good reduction at all odd primes (see the proof of [8, Proposition 4.2]). As before this is just saying that $y = \pm 1$ and $z = \pm 1$. We immediately see that $y = 1$ and $z = 1$ (since $k = 3$). We may thus assume that $p \equiv 3 \pmod 4$.

Proposition 4.3 of [8] shows that the image of ρ is isomorphic to the normalizer of the non-split Cartan subgroup. Then Theorem 8.1 of [8] shows that the j-invariant of E belongs to $\mathbb{Z}[\frac{1}{p}]$. Moreover, p does not divide yz by the same argument as in the proof of [8, Corollary 4.4]. Hence we know that j is in $\mathbb{Z}$, and from Lemma 3 above we know that $y = z = 1$ as required.

2.4. Exceptions to Theorem 1; the cases $p < 7$ and $k = 1$. The reader will probably be wondering where our proof fails for the cases $p < 7$ and $k = 1$. For $p < 7$ we are unable to prove the irreducibility of the Galois representation ρ. For $k = 1$ the Serre conductor of ρ is 128, and we know that the dimension of $S_2(\Gamma_0(128))$ is 9. So far as we know, there are as of yet no methods developed to deal with cases where the dimension after level-lowering is greater than 1.

3. Special Cases

3.1. The equation $x^2 + 2^k = y^n$. In [5] J.H.E. Cohn shows, for k odd, that the equation

$$x^2 + 2^k = y^n, \qquad x, y \text{ integers}, n \geq 3, \tag{5}$$

has only the following solutions in positive integers x, y with $n \geq 3$

k	x	y	n
$6\alpha+1$	$5\cdot 2^{3\alpha}$	$3\cdot 2^{2\alpha}$	3
$4\alpha+5$	$7\cdot 2^{2\alpha}$	$3\cdot 2^{\alpha}$	4
$10\alpha+5$	$11\cdot 2^{5\alpha+3}$	$3\cdot 2^{2\alpha+1}$	5

for $\alpha \geq 0$.

The case with k even has proved to be more troublesome. In [1] Arif and Abu Muriefah made a plausible conjecture as to the solutions with $k = 2m$. Cohn [6] proves the conjecture for most values of m less than 1000, including all those less than 100. Equation (5) is of course a special case of (1) corresponding to the case $z = -1$ provided that $n = p$ is an odd prime. It turns out that our Theorem 1 is enough to complete the resolution of (5).

Theorem 2. *(Conjecture of Arif and Abu Muriefah) If $n \geq 3$, $k = 2m$, the diophantine equation (5) has precisely two families of solutions given by $x = 2^m$ for all m, and by $n = 3$, $x = 11 \cdot 2^{3M}$ if $m = 3M + 1$.*

Proof. We shall use the results of [1], [6] to reduce the theorem to a special case of Theorem 1. It is shown in [1, page 300] that n must be odd, and that there are no further solutions with x, y even. It is enough therefore to show that there are no solutions to the equation

$$x^2 + 2^{2m} = y^p \tag{6}$$

for $m \geq 0$, $p \geq 3$ prime, and x, y odd integers. However Cohn showed that any such solution to equation (6) must satisfy $m \geq 100$ ([6, page 462]) and $p \equiv 1, 4, 7 \pmod 9$ ([6, Lemma 3]). In particular, any such solution will be a solution to equation (1) with $p \geq 7$, $z = -1$ and $k = 2m \geq 200$. This contradicts Theorem 1. $\square$

Remark. M. Le has just published a solution to equation (6) using linear forms in logarithms (see [13]).

3.2. The equation $x^2 - 2^k = y^n$.

The equation

$$x^2 - 2^k = y^n, \qquad x, y, k, n \in \mathbb{N},\ \gcd(x, y) = 1,\ y > 1,\ n \geq 3, \tag{7}$$

has been considered by Bugeaud [3] and by Guo and Le [10]. In particular, Bugeaud showed that if x, y, k, n is a solution satisfying the above conditions then,

- n and k are odd; this was shown using elementary factorization arguments.
- $n \leq 7.3\times 10^5$; this was established using lower bounds for linear forms in logarithms.

While we are unable to resolve equation (7) completely, our Theorem 1 implies the following.

Theorem 3. *If the equation (7) has a solution satisfying the above conditions then either $k = 1$ or $n = 3^a 5^b$ for some a, b.*

We note in passing that it maybe possible to eliminate the case $n = 3^a 5^b$ from the theorem as follows. Clearly it is sufficient to solve the equations

$$x^2 - 2^k = y^3 \qquad \textit{and} \qquad x^2 - 2^k = y^5.$$

Now k must be odd by the result quoted above, and this leads us to factorize the left-hand side of each equation over $\mathbb{Q}(\sqrt{2})$. We can reduce each equation to a set of Thue-Mahler equations, and these can be solved using standard methods as in [16, Chapter VIII], although we have not attempted to do this. We do not see how the equation $x^2 - 2 = y^n$ (corresponding to $k = 1$) can be solved using existing methods.

Acknowledgment. I am deeply indebted to the referee and Professor Bjorn Poonen for many useful comments and corrections, and particularly for the suggestion that my method can deal with equation (1) and not just the equation (5).

References

[1] S. A. Arif, F. S. Abu Muriefah, *On the diophantine equation $x^2 + 2^k = y^n$*. Internat. J. Math. & Math. Sci. **20** no. **2** (1997), 299–304.

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

[3] Y. Bugeaud, *On the diophantine equation $x^2 - 2^m = \pm y^n$*. Proc. Amer. Math. Soc. **125** (1997), 3203–3208.

[4] J.E. Cremona, *Algorithms for modular elliptic curves* (second edition). Cambridge University Press, 1996.

[5] J. H. E. Cohn, *The diophantine equation $x^2 + 2^k = y^n$*. Arch. Math. **59** (1992), 341–344.

[6] J. H. E. Cohn, *The diophantine equation $x^2 + 2^k = y^n$, II.* Internat. J. Math. & Math. Sci. **22** no. **3** (1999), 459–462.

[7] H. Darmon, *The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$*. International Mathematics Research Notices **10** (1993), 263–274.

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

[9] F. Diamond, *On deformation rings and Hecke rings.* Ann. Math. **144** no. **1** (1996), 137–166.

[10] Y. Guo, M. Le, *A note on the exponential diophantine equation $x^2 - 2^m = y^n$*. Proc. Amer. Math. Soc. **123** (1995), 3627–3629.

[11] W. Ivorra, *Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$*. To appear in Acta Arith.

[12] A. W. Knapp, *Elliptic curves.* Mathematical Notes **40**, Princeton University Press, 1992.

[13] M. Le, *On Cohn's conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$*, Arch. Math. **78** no. **1** (2002), 26–35.

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

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

[16] N.P. Smart, *The algorithmic resolution of diophantine equations.* LMS Student Texts **41**, Cambridge University Press, 1998.

[17] R. TAYLOR, A. WILES, *Ring-theoretic properties of certain Hecke algebras*. Ann. Math. **141** (1995), 553–572.

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

Samir SIKSEK
Department of Mathematics and Statistics
College of Science
Sultan Qaboos University
P.O. Box 36
Al-Khod 123, Oman
E-mail : siksek@squ.edu.om