ON THE DIOPHANTINE EQUATION $x^2 + 7 = y^m$

SAMIR SIKSEK AND JOHN E. CREMONA

ABSTRACT. In this paper we study the equation $x^2+7 = y^m$, in integers x, y, m with $m \geq 3$, using a Frey curve and Ribet's level lowering theorem. We adapt some ideas of Kraus to show that there are no solutions to the equation with m composite and $m > 15$, and none with m prime and $11 \leq m < 10^8$.

1. Introduction

In [6, page 380] J.H.E. Cohn makes the challenge of proving the following:

Conjecture 1. *The only solutions to the equation*

$$x^2 + 7 = y^m \tag{1}$$

with $x, y, m \in \mathbb{Z}$ and $m \geq 3$ are the following:

m	x	y	m	x	y	m	x	y
3	± 1	2	3	± 181	32	4	± 3	± 2
5	± 5	2	5	± 181	8	7	± 11	2
15	± 181	2						

It is known that there are no other solutions with y odd, nor with m even, nor with $3|m$ (see [6, page 380]). In [12] Lesage proves various partial results concerning the equation (1), including the following.

- There are no solutions to equation (1) with $m = 5, 7, 13$ apart from those listed in the table above. This he proves by reducing to Thue equations (see the next section), which he then solves by hand.
- There are no solutions to equation (1) for $m = 11$ and for m prime and $17 \leq m \leq 5000$. This he proves using classical algebraic number theory, and a computational method.
- If (x, y, m) is a solution to (1) then $m \leq 6.6 \times 10^{15}$. This he proves using lower bounds for linear forms in logarithms.

It is clearly sufficient to restrict attention to the equation

$$x^2 + 7 = y^p \tag{2}$$

where p is prime. In this note we prove the following.

Theorem 2. *Equation (2) has no solutions with p prime and $11 \leq p \leq 10^8$.*

2000 *Mathematics Subject Classification.* Primary 11G30, Secondary 11D41.

Key words and phrases. Diophantine equations, Frey curves.

The first author's work is funded by a grant from Sultan Qaboos University (IG/SCI/DOMS/02/06).

In fact we give a practical criterion for the non-existence of solutions to (2) for any particular prime $p \geq 11$. Our proof of Theorem 2 comes down to the use of a computer program to check the criterion for $11 \leq p \leq 10^8$.

We note that our result is still a far way off from Lesage's bound of 6.6×10^{15} quoted above. However, since 10^8 is greater than the square-root of 6.6×10^{15}, the following corollary is immediate.

Corollary 3. *Equation (1) has no solutions with m composite, apart from those listed in the above table. Indeed, if (x, y, m) is any solution to (1) not listed above, then m is a prime satisfying $10^8 < m < 6.6 \times 10^{15}$.*

Finally we discuss the possibility of completely resolving equation (1) using the method of this paper. This will have to wait until substantial improvements are made in lower bounds for linear forms in three logarithms.

2. The cases $m = 3, 5, 7$

In this section we show that there are no solutions to equation (1) when $m = 3,\ 5,\ 7$ except those listed in the table above. As indicated in the introduction, these cases are already covered by the literature. We have however decided to give a very concise treatment of these cases for two reasons. First, our treatment illustrates the power of the computer algebra packages used; what previously involved several pages of computation is now practically effortless. Secondly, it also makes our approach to (1) almost independent of the previous literature on this equation; we will only assume henceforth that y is even (and refer to [13] for a proof of this). The case m even can be safely left to the reader.

Let $\rho = (1 + \sqrt{-7})/2$; then $1, \rho$ is a basis for the ring of integers of the field $\mathbb{Q}(\sqrt{-7})$. A standard factorization argument leads us to consider

$$\frac{x-1}{2} + \rho = \rho^{m-2}(U + \rho V)^m$$

with $U,\ V$ integers. Comparing the coefficients of ρ for $m = 3, 5, 7$ we obtain the following Thue equations:

$$U^3 + 3U^2V - 3UV^2 - 3V^3 = 1,$$

$$-U^5 - 15U^4V - 10U^3V^2 + 50U^2V^3 + 35UV^4 - 3V^5 = 1$$

and

$$-U^7 + 35U^6V + 147U^5V^2 - 105U^4V^3 - 595U^3V^4 - 231U^2V^5 + 161UV^6 + 45V^7 = 1$$

respectively. Fortunately the algebraic number theory package `KANT` (see [7]) has routines for solving Thue equations; these are also available in Magma (see [3]). Using either of these packages, we find that the only solutions to the first equation are $(U, V) = (1, 0), (-2, 3)$, the only solutions to the second equation are $(U, V) = (-1, 0), (2, -1)$, and the only solutions to the third equation are $(U,V)=(-1,0)$. These respectively give the following solutions for (1):

$$(m,x,y)=(3,\pm 1,2),(3,\pm 181,32),(5,\pm 5,2),(5,\pm 181,8),(7,\pm 11,2),$$

as required.

3. The Frey Curve and Level-Lowering

In this section we associate a Frey curve to any putative solution of our equation (2). For a general approach of how to associate Frey curves to ternary Diophantine equations we refer the reader to a useful recent paper of Bennett and Skinner [2]. Our approach is however self-contained in this regard.

Suppose $p \geq 11$ is prime and $x,\ y$ are integers satisfying equation (2), and the conditions:

$$x \equiv 1 \pmod 4 \qquad \text{and} \qquad y \text{ is even.} \tag{3}$$

There is no loss of generality in making this assumption, as we know from the comments made in the introduction that y must be even and so x odd, and we can replace x by $-x$, if necessary, to get $x \equiv 1 \pmod 4$.

We associate to this solution the 'Frey curve':

$$E_{x,y}: \qquad Y^2 = X^3 + xX^2 + \frac{y^p}{4}X. \tag{4}$$

Lemma 4. *$E_{x,y}$ has the global minimal model*

$$Y^2 + XY = X^3 + \frac{(x-1)}{4}X^2 + \frac{y^p}{64}X. \tag{5}$$

Its minimal discriminant and conductor respectively are

$$\Delta = \frac{-7y^{2p}}{2^{12}}, \qquad N = 14 \prod_{\substack{l \text{prime} \\ l \mid y,\ l \neq 2,7}} l. \tag{6}$$

Proof. This follows easily from Tate's algorithm. ☐

We now come to level-lowering. Let E be the following elliptic curve over $\mathbb{Q}$:

$$E: \quad Y^2 + XY + Y = X^3 + 4X - 6;$$

this is curve 14A1 in [5]. Write ρ_p for the Galois representation

$$\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$$

on the p-torsion of E, and let $\rho_p^{x,y}$ be the corresponding Galois representation on the p-torsion of $E_{x,y}$. If l is a prime, let $a_l(E)$ be the trace of Frobenius of the curve E at l, and let $a_l(E_{x,y})$ denote the corresponding trace of Frobenius of $E_{x,y}$.

Lemma 5. *With x,y,p as above, the Galois representations $\rho_p^{x,y}$, ρ_p are isomorphic. Moreover,*

(i) $a_l(E_{x,y}) \equiv a_l(E) \pmod{p}$ *if l is a prime of good reduction for both curves.*

(ii) $a_l(E_{x,y})a_l(E) \equiv l+1 \pmod{p}$ *if $l \neq 2, 7$ and $l|y$.*

Proof. By the work of Wiles and others [4] the curve $E_{x,y}$ is modular. Moreover, by Lemma 4, it is semi-stable. Thus by a theorem of Mazur [14, Theorem 4] the Galois representation $\rho_p^{x,y}$ on the p-torsion is surjective (recall $p \geq 11$). Applying Ribet's 'level lowering' theorem [15], we see that $\rho_p^{x,y}$ is isomorphic to some representation ρ of weight 2 and level 14. However $S_2(\Gamma_0(14))$ has dimension 1. Moreover, the curve E is (up to isogeny) the unique curve of conductor 14. It follows that $\rho = \rho_p$ is the Galois representation on the p-torsion of the curve E. The rest of the lemma follows from [10, Proposition 3]. □

4. The Method of Kraus

In this section we mimic Kraus's approach (see [9]) to solving the equation $a^3 + b^3 = c^p$. We explain the idea briefly. Suppose $p \geq 11$ is a given prime, and we would like to prove the non-existence of solutions to equation (2). Choose a small integer n such that $q = np + 1$ is also prime. Suppose (x, y) is a solution to (2). Then working modulo q we see that $x^2 + 7 = y^p$ is either 0 or an n-th root of unity. Since n is small, we can list all such $x \pmod{q}$. We compute $a_q(E)$, and $a_q(E_{x,y})$ for each x, and may then find that for no x in our list are the relations in Lemma 5 satisfied. If this is the case then we have a contradiction, and we deduce that there are no solutions to (2) for the given prime p.

We now write this more formally. Suppose q is a prime number satisfying $q \equiv 1 \pmod{p}$, and write $q = np + 1$. Let

$$\mu_n(\mathbb{F}_q) = \left\{ \zeta \in \mathbb{F}_q^* \quad : \quad \zeta^n = 1 \right\}.$$

Define

$$A(n, q) = \left\{ \zeta \in \mu_n(\mathbb{F}_q) \quad : \quad \left(\frac{\zeta - 7}{q} \right) = 0 \text{ or } 1 \right\}.$$

For each $\zeta \in A(n, q)$, let δ_ζ be an integer satisfying

$$\delta_\zeta^2 \equiv \zeta - 7 \pmod{q}.$$

Let $a_q(\zeta)$ be the trace of Frobenius of the curve

$$E_\zeta : Y^2 = X^3 + \delta_\zeta X^2 + \frac{\zeta}{4} X$$

defined over $\mathbb{F}_q$. (Nonsingularity of this curve is easily checked, since $q > 7$.) We can now state our sufficient condition for the insolubility of (2).

Theorem 6. *Let E be the curve defined above. Let p be a prime number ≥ 11. Suppose that there exists an integer $n \geq 2$ satisfying the following:*

(a) *The integer $q = np + 1$ is a prime.*

(b) *Either $a_q(E)^2 \not\equiv 4 \pmod{p}$, or $\left(\frac{-7}{q}\right) = -1$.*

(c) *For all* $\zeta \in A(n,q)$, *we have*

$$a_q(\zeta)^2 \not\equiv a_q(E)^2 \pmod{p}.$$

Then the equation $x^2+7=y^p$ *does not have any solutions in integers.*

Proof. Suppose that (a),(b),(c) are satisfied and that the equation $x^2+7=y^p$ does have a solution (x,y). We suppose without loss of generality that the condition (3) is satisfied, and we let $E_{x,y}$ be the curve defined in the previous section.

Now let $q=np+1$ be as in the statement of the theorem. First we claim that $q \nmid y$. Suppose that $q|y$. From (2) we see that $\left(\frac{-7}{q}\right)=1$. Thus from condition (b) we see that $a_q(E) \not\equiv \pm 2 \pmod{p}$. But $q|y$ implies that q is a prime of multiplicative reduction for $E_{x,y}$. Hence ([8, p. 295]) $a_q(E_{x,y})=\pm 1$. From Lemma 5(ii)

$$a_q(E) \equiv \pm(q+1) \equiv \pm 2 \pmod{p}.$$

This contradiction shows that $q \nmid y$, and so q is a prime of good reduction for both curves. Clearly there is some $\zeta \in A(n,q)$ such that

$$y^p \equiv \zeta \pmod{q}, \qquad \text{and} \quad x \equiv \pm\delta_\zeta \pmod{q}.$$

It follows that $a_q(E_{x,y}) = \pm a_q(\zeta)$. Moreover $a_q(E_{x,y}) \equiv a_q(E) \pmod{p}$, from Lemma 5(i). Thus $a_q(E) \equiv \pm a_q(\zeta)(\pmod{p})$ contradicting condition (c) of the theorem. Hence there is no solution to (2). □

5. The Computation

We wrote a simple program using the package Pari/GP (see [1]) to test whether a given prime p satisfies the conditions of the Theorem, by finding a suitable integer n. Using this program we verified that the equation (2) has no solutions for all primes p satisfying $11 < p < 10^8$, and also for all p in the ranges $10^k < p < 10^k + 1000$ for $8 \le k \le 20$. In the range $p < 10^8$, the largest value of n needed was $n = 284$ for $p = 73342163$; this computation took about 4 days on an 850MHz AMD Athlon.

Details may be obtained from `http://www.maths.nott.ac.uk/personal/jec/ftp/progs`: the program itself is in the file `eqn_x27yp.gp`, and the output giving a suitable value of n for each of the 5761451 primes p in the range $11 \le p < 10^8$ is in `eqn_x27yp.out` (which is 5761451 lines long!).

6. Epilogue

Suppose P is a polynomial with rational coefficients and at least two distinct roots. A theorem of Schinzel and Tijdeman [16] states there is an effectively computable constant $c(P)$ such that if $x,\ y,\ m$ are integers with $|y|>1, m>1$, satisfying

$$P(x) = y^m$$

then $m < c(P)$. The constant here depends on the constants appearing in effective lower bounds for linear forms in logarithms.

To obtain a reasonable bound for m in our equation (1) we need a good lower bound for linear forms in three (complex) logarithms. It seems to us that the bounds in the literature (e.g. [17]) will not give us a bound on m that is much sharper than Lesage's bound quoted in the introduction, and this is clearly out of reach of our computational method. However it is our hope that bounds for linear forms in three logarithms will be improved as bounds for linear forms in two logarithms have been improved [11]. It may then be possible to completely settle equation (1) (and so establish Cohn's conjecture) using the method of this paper.

Acknowledgment. We are indebted to the referee for pointing out to us the papers of Lesage [12] and of Bennett and Skinner [2].

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP*, version 2.1.1. (See also `http://www.parigp-home.de/`.)

[2] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, to appear in the Canadian Journal of Mathematics.

[3] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au:8000/u/magma/`.)

[4] 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 No.4** (2001), 843–939.

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.

[6] J. H. E. Cohn, *The Diophantine equation $x^2 + C = y^n$*, Acta Arith. **LXV.4** (1993), 367–381.

[7] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *Kant V4*, J. Symbolic Comp. **24** (1997), 267–283. (See also `http://www.math.TU-Berlin.DE/algebra/`.)

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

[9] A. Kraus, *Sur l'équation $a^3 + b^3 = c^p$*, Experimental Mathematics **7** (1998), No. 1, 1–13.

[10] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

[11] M. Laurent, M. Mignotte and Y. Nesterenko, *Formes linéares en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 255–265.

[12] J.-L. Lesage, *Différence entre puissances et carrés d'entiers*, Journal of Number Theory **73** (1998), 390–425.

[13] W. Ljunggren, *On the diophantine equation $Cx^2 + D = y^n$*, Pacific J. Math. **14** (1964), 585–596.

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

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

[16] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. **XXXI** (1976), 199–204.

[17] M. Waldschmidt, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canadian J. Math. **45** (1993), 176-224.

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

School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, UK.
E-mail address: John.Cremona@nottingham.ac.uk