Indag. Mathem., N.S., 18 (4), 507–525 December 17, 2007

# The Diophantine equation $(x^k - 1)(y^k - 1) = (z^k - 1)^t$

by Michael A. Bennett [1]

*Department of Mathematics, University of British Columbia, Vancouver, BC*

Communicated by Prof. R. Tijdeman at the meeting of October 28, 2006

ABSTRACT

We sharpen work of Bugeaud to show that the equation of the title has, for $t = 1$ or 2, no solutions in positive integers $x$, $y$, $z$ and $k$ with $z > 1$ and $k > 3$. The proof utilizes a variety of techniques, including the hypergeometric method of Thue and Siegel, as well as an assortment of gap principles.

## 1. INTRODUCTION

The problem of understanding the distribution of integer "points" on surfaces is currently in its relative infancy, at least in comparison to analogous questions for curves. In few cases can we say anything definitive and, in many situations, even conjectural information is lacking. For certain surfaces, however, the techniques of Diophantine approximation enable one to deduce fairly complete answers to such questions; we will consider such a pair of surfaces here.

The Diophantine equations

$$(1.1) \qquad (x^2 - 1)(y^2 - 1) = (z^2 - 1)$$

and

$$(1.2) \qquad (x^2 - 1)(y^2 - 1) = (z^2 - 1)^2$$

*MSC:* Primary 11D45, 11D61; Secondary 11J82, 11J86

E-mail: bennett@math.ubc.ca (M.A. Bennett).

[1] The author was supported in part by a grant from NSERC.

provide accessible examples of equations possessing infinitely many (nontrivial) solutions in integers, arising in a somewhat interesting manner. In the first case, all solutions may be derived from the trivial solution $(1, n, 1)$, via a construction that is analogous to that used to deduce the "tree" of solutions to the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

In the case of equation (1.2), it is still an open question to find all integral points on the corresponding surface. If we assume $2 \leqslant x < y$, then one infinite family is given by taking

$$(x, y, z) = (P_{2k}, P_{2k+2}, P_{2k+1}), \quad k \geqslant 1,$$

where the sequence $P_j$ is defined by

$$P_0 = P_1 = 1, \qquad P_{n+2} = 2P_{n+1} + P_n, \quad \text{for } n \geqslant 0.$$

Three solutions outside this family are

$$(x, y, z) \in \{(2, 97, 13), (4, 31, 11), (155, 48049, 2729)\}.$$

A number of generalizations of equations (1.1) and (1.2) have been considered in the literature. Solving equation (1.1), for instance, is equivalent to the problem of determining positive integers $a$ and $b$ such that $\{1, a, b\}$ is a *Diophantine triple*. Recall that we call a set of positive integers $\{a_1, a_2, \ldots, a_m\}$ a *Diophantine m-tuple* if $a_i a_j + 1$ is a square for each $1 \leqslant i < j \leqslant m$. Similarly, equation (1.2) may be restated as the question of finding positive integers $a, b$ and $c$ such that each of $ab^2 + 1, ac^2 + 1$ and $abc + 1$ is a perfect square. The reader is directed to [14] for more background and the current state-of-affairs for these problems.

From such a perspective, in a recent paper, Bugeaud [9] considered the problem of finding positive integers $a$ and $b$ such that one of the sets $\{a + 1, b + 1, ab + 1\}$ or $\{a + 1, ab + 1, ab^2 + 1\}$ is comprised entirely of perfect $k$th powers, for $k \geqslant 3$. These correspond, respectively, to the Diophantine equations

$$(1.3) \qquad (x^k - 1)(y^k - 1) = (z^k - 1)$$

and

$$(1.4) \qquad (x^k - 1)(y^k - 1) = (z^k - 1)^2,$$

where, in the latter case, Bugeaud made the additional assumption that the smaller of $x^k - 1$ or $y^k - 1$ divides $z^k - 1$. He showed (Theorem 1 of [9]) that there are no solutions to (1.3) with $z \geqslant 2$, provided $k \geqslant 75$, or if $k \geqslant 5$ and the smaller of $x$ and $y$ is sufficiently large. He further obtained somewhat weaker results for equation (1.4) (see Theorem 2 of [9]).

In this paper, we will prove the following pair of theorems

**Theorem 1.1.** *The equation*

$$(x^k - 1)(y^k - 1) = (z^k - 1)$$

*has only the solutions*

$$(x, y, z, k) = (-1, 4, -5, 3) \text{ and } (4, -1, -5, 3)$$

*in integers $x, y, z$ and $k$ with $|z| \geqslant 2$ and $k \geqslant 3$.*

**Theorem 1.2.** *The equation*

$$(x^k - 1)(y^k - 1) = (z^k - 1)^2$$

*has no solutions in integers $x$, $y$, $z$ and $k$ with $x \neq \pm y$, $|z| \geqslant 2$ and $k \geqslant 4$.*

Note that we have not assumed, as was done in [9], that the variables $x, y$ and $z$ are positive integers. In light of our earlier remarks about equations (1.1) and (1.2), Theorem 1.1 is best possible, while Theorem 1.2 is nearly so. We are, however, unable to treat equation (1.4) in case $k = 3$.

The main reason for the sharpness of Theorems 1.1 and 1.2, relative to those of [9], is somewhat surprising. The results of [9] are proved by combining lower bounds for linear forms in the complex logarithms of algebraic numbers, with explicit irrationality measures for algebraic numbers, stemming from the "hypergeometric method" of Thue and Siegel. In what follows, a key observation is that the first of these techniques is not only unnecessary (in all but a single case), at least in this context, but even leads to weaker results. To treat small values of $k$ (such as $k = 3$ and $k = 4$ in equation (1.3), where Bugeaud's techniques fail), we further introduce some new "gap principles" (to guarantee that $|x - y|$ is not too small). In one case, switching from consideration of positive integers to the more general case makes life much more difficult for us. Specifically, to handle the situation where, say, $x = -1$ in Theorem 1.1, requires the solution of a family of Thue equations of arbitrarily high degree. We accomplish this by sharpening earlier work of the author on rational approximation to algebraic numbers via the hypergeometric method of Thue and Siegel, together with a method for binomial Thue equations based upon the theory of Frey curves and associated Galois representations.

## 2. PROOFS

Our arguments begin by following similar lines to those of [9]. From a putative solution to one of (1.3) or (1.4), we will deduce the existence of a good rational approximation to a particular algebraic number of degree $k$. Since this algebraic number takes the form $\sqrt[k]{m^k \pm 1}$, classical work of Thue, with a few modern "bells and whistles", enables us to derive a contradiction, as long as $|x - y|$ is much larger than $\min\{|x|, |y|\}$.

We begin by noting that proving Theorem 1.1 reduces to consideration of either equation (1.3) with $k = 4$ or $k$ an odd prime, or to one of the equations

$$(2.1) \qquad (x^k + 1)(y^k + 1) = (z^k - 1),$$

or

$$(2.2) \qquad (x^k + 1)(y^k - 1) = (z^k + 1),$$

where $k$ is an odd prime, and, in all cases, $x$, $y$ and $z$ may be taken to be *positive* integers. Similarly, equation (1.4) in arbitrary integers may be reduced to one of (1.4) (with $k = 4$, $k = 6$, or $k \geqslant 5$ prime),

$$(2.3) \qquad (x^k - 1)(y^k - 1) = (z^k + 1)^2,$$

$$(2.4) \qquad (x^k + 1)(y^k + 1) = (z^k - 1)^2,$$

or

$$(2.5) \qquad (x^k + 1)(y^k + 1) = (z^k + 1)^2.$$

In each of these last three cases, $k \geqslant 5$ is taken to be prime, while, in all four cases, we assume that $x$, $y$ and $z$ are positive integers.

We begin by discussing in detail how to treat equation (1.3), for positive integers $x, y, z$. Afterwards, we will indicate where changes need to be made to our proof to handle the remaining equations (1.4), (2.1), (2.2), (2.3), (2.4) and (2.5).

Let us suppose, then, for the next few sections, that we have a solution to equation (1.3) in positive integers $x, y, z$ and $k$ with $z \geqslant 2$ and $k \geqslant 3$. We may suppose, without loss of generality, that

$$y \geqslant x > 1$$

and, as mentioned previously, that either $k = 4$ or that $k \geqslant 3$ is prime. We begin by deriving a result that guarantees that $y$ must be, in fact, much larger than $x$ (sharpening Lemma 1 of [9]). Let us write

$$(2.6) \qquad a + 1 = x^k, \qquad b + 1 = y^k, \qquad ab + 1 = z^k.$$

It follows that $z = xy - t$ for $t$ a positive integer, that is

$$\left((ab + 1)^{1/k} + t\right)^k = (a + 1)(b + 1).$$

Expanding this, we have

$$k(ab + 1)^{(k-1)/k}t + \binom{k}{2}(ab + 1)^{(k-2)/k}t^2 + \cdots + k(ab + 1)^{1/k}t^{k-1} + t^k = a + b.$$

We claim that $a < (ab+1)^{(k-2)/k}$. If $k \geqslant 4$, this is immediate from the inequality $b \geqslant a$. If $k = 3$ and $a \geqslant (ab+1)^{1/3}$, then $b < a^2$, contradicting

$$3(ab)^{2/3} < 3(ab+1)^{2/3} < a + b \leqslant 2b.$$

It therefore follows, in all cases, that we have

$$k(ab)^{(k-1)/k}t < k(ab+1)^{(k-1)/k}t < b$$

and so

$$b > k^k a^{k-1} t^k. \tag{2.7}$$

Next note that from (2.6), we have

$$\left(\frac{xy}{z}\right)^k - \frac{a+1}{a} = \frac{a^2-1}{a(ab+1)} < \frac{a}{z^k},$$

whence

$$\left|\sqrt[k]{1+\frac{1}{a}} - \frac{xy}{z}\right| < \frac{a}{kz^k}. \tag{2.8}$$

To deduce a lower bound which will contradict (2.8), we appeal to an old result of the author (Theorem 1.3 of [4]). This is, as stated, reasonably easy to derive from Thue's original work [23]. Defining

$$\mu_n = \prod_{p|n} p^{1/(p-1)},$$

we have

**Theorem 2.1** ([4]). *If $k$ and $a$ are positive integers with $k \geqslant 3$ and*

$$\left(\sqrt{a} + \sqrt{a+1}\right)^{2(k-2)} > (k\mu_k)^k \tag{2.9}$$

*then*

$$\left|\sqrt[k]{1+\frac{1}{a}} - \frac{p}{q}\right| > (8k\mu_k a)^{-1} q^{-\lambda}$$

*with*

$$\lambda = 1 + \frac{\log(k\mu_k(\sqrt{a}+\sqrt{a+1})^2)}{\log(\frac{1}{k\mu_k}(\sqrt{a}+\sqrt{a+1})^2)}. \tag{2.10}$$

From the fact that $a = x^k - 1$, it is easy to show that (2.9) is satisfied except for

$$(x,k) \in \{(2,3),(3,3),(2,4),(2,5)\}. \tag{2.11}$$

For the time being, we will suppose that $(x, k)$ is outside this set (so that $\lambda < k$). Then combining (2.8) with Theorem 2.1 yields

$$z^{k-\lambda} < 8\mu_k a^2 \tag{2.12}$$

and hence,

$$b^{k-\lambda} < 8^k \mu_k^k a^{k+\lambda}. \tag{2.13}$$

If $k \geqslant 7$ is prime, then $\mu_k = k^{1/(k-1)}$. Since $a = x^k - 1$, from equation (2.10), it is not hard to see that $\lambda$ is monotone decreasing in $x \geqslant 2$ and $k \geqslant 7$, whereby $\lambda < 3.15$. Hence (2.13) implies that $b < 80a^{2.7}$, contradicting (2.7). Similarly, if $k = 5$ and $x \geqslant 3$, then $\lambda < 2.8$, and so $b < 282\, a^{3.6}$. Again, this contradicts (2.7). If, however, $k = 5$ and $a = 31$, then we have

$$31y^5 - z^5 = 30 \tag{2.14}$$

and hence

$$\left| \sqrt[5]{31} - \frac{z}{y} \right| < \frac{30^{1/5}}{5y^5}.$$

On the other hand, from Corollary 1.2 of [4],

$$\left| \sqrt[5]{31} - \frac{z}{y} \right| > \frac{0.01}{y^{2.83}}.$$

We thus have

$$y^{2.17} < 20 \cdot 30^{1/5}$$

and so $y < 6$. Since (2.14) implies that $y$ is coprime to 30, it follows that $y = 1$, a contradiction.

### 3. THE CASE $k = 4$

Let us now suppose that $k = 4$. We begin by introducing a "gap principle" that sharpens inequality (2.7) in this case. It is worth noting that, in the next section (where we treat $k = 3$) yet another, even stronger gap principle is produced which may, in fact, be adapted to the case $k = 4$.

After a little work, from (2.7), we reach the inequality

$$y > 3x^3 t. \tag{3.1}$$

Our initial goal is to show that

$$b > 16a^4. \tag{3.2}$$

From $z = xy - t$, we have

$$(x^4 - 1)(y^4 - 1) = (xy - t)^4 - 1$$

and so

$$4x^3y^3t + 4xyt^3 + 2 = x^4 + y^4 + 6x^2y^2t^2 + t^4 \tag{3.3}$$

and hence

$$4xyt^3 + 2 \equiv x^4 + 6x^2y^2t^2 + t^4 \pmod{y^3}. \tag{3.4}$$

We will use these relations to show that $t > x/2$. If we have

$$4xyt^3 + 2 = x^4 + 6x^2y^2t^2 + t^4,$$

then (3.3) implies that $y = 4x^3t$ and hence that $x^4$ divides $t^4 - 2$ (so that $t > x$). Otherwise, we have from (3.4) that either

$$4xyt^3 + 2 \geqslant x^4 + 6x^2y^2t^2 + t^4 + y^3$$

or

$$4xyt^3 + 2 + y^3 \leqslant x^4 + 6x^2y^2t^2 + t^4.$$

In the first case, $4xyt^3 > y^3$ and hence, from (3.1), $t > 9x^5/4$. The second inequality, together with (3.1), implies that $y^3 < 6x^2y^2t^2$ and hence that $y < 6x^2t^2$. Combining this with (3.1) implies that $t > x/2$, as claimed. We may thus conclude, from (2.7), that

$$b > 4^4a^3t^4 > 16a^3x^4 > 16a^4,$$

as desired.

If $x \geqslant 3$, combining (2.13) and (3.2), we find that

$$a^{12-5\lambda} < 16^{\lambda},$$

contradicting (2.10) provided $x \geqslant 35$ (i.e. $a \geqslant 1500624$).

For $2 \leqslant x \leqslant 34$, we argue somewhat more carefully. If $x = 2$ (so that $a = 15$), we have

$$15y^4 - z^4 = 14$$

and so

$$\left| \sqrt[4]{15} - \frac{z}{y} \right| < \frac{14^{1/4}}{4y^4}.$$

On the other hand, Corollary 1.2 of [4] implies that

$$\left|\sqrt[4]{15} - \frac{z}{y}\right| > \frac{0.03}{y^{3.27}},$$

and so it follows that $y \leqslant 45$ and hence, from (3.1), $t = 1$, contradicting $t > x/2$.

For $3 \leqslant x \leqslant 34$, the inequality $z^{4-\lambda} < 16a^2$ implies, in each case, that $z < 10^8$. From

$$(x^4 - 1)y^4 - z^4 = x^4 - 2,$$

it follows that

$$\left|\sqrt[4]{x^4 - 1} - \frac{z}{y}\right| < \frac{(x^4 - 2)^{1/4}}{4y^4}$$

and so, from (3.1) and the inequality $t > x/2$, we have that $z/y$ is a convergent in the continued fraction expansion to $\sqrt[4]{x^4 - 1}$, say $z/y = p_j/q_j$ where, additionally, since

$$z/y < \sqrt[4]{x^4 - 1},$$

$j$ is even. Here and henceforth, we write

$$\sqrt[k]{a} = [a_0, a_1, a_2, \ldots] \quad \text{and} \quad p_i/q_i = [a_0, \ldots, a_i],$$

where the $a_i$ denote the partial quotients in the infinite simple continued fraction expansion to $\sqrt[k]{a}$ and the $p_i/q_i$ the corresponding convergents. Since, from the classical theory of continued fractions (see e.g. [18], Theorem 9.6),

$$\left|\sqrt[4]{x^4 - 1} - \frac{p_j}{q_j}\right| > \frac{1}{(a_{j+1} + 2)q_j^2},$$

we have that

$$9x^8 < 4y^2 < (a_{j+1} + 2)(x^4 - 2)^{1/4}$$

and hence

$$a_{j+1} > 9x^7 - 2 \geqslant 19681. \tag{3.5}$$

We calculate that, in each case, $p_{13} > 10^8$, while inequality (3.5) is never satisfied, for even $j < 20$. This completes the proof of Theorem 1.1, in case $k = 4$.

## 4. THE CASE $k = 3$

It remains to treat equation (1.3) when $k = 3$. We begin by introducing a new method for sharpening inequality (2.7). This has its genesis in the arguments at the end of the preceding section. From the equation

$$ay^3 - z^3 = a - 1$$

it follows that

$$\left|\sqrt[3]{a} - \frac{z}{y}\right| < \frac{(a-1)^{1/3}}{3y^3}. \tag{4.1}$$

Since (2.7) implies that $y^3 > b > 27a^2$, whence $y > 3a^{2/3}$, $z/y$ is necessarily a convergent in the continued fraction expansion to $\sqrt[3]{a}$, say $z/y = p_j/q_j$ with, since $z/y < \sqrt[3]{a}$, $j$ even. Moreover, from the inequality

$$\left|\sqrt[3]{a} - \frac{p_j}{q_j}\right| > \frac{1}{(a_{j+1}+2)q_j^2},$$

we have that

$$3a^{2/3} < y < (a_{j+1}+2)(a-1)^{1/3}$$

and hence, since $a = x^3 - 1$,

$$a_{j+1} > 3x - 2 \geqslant 4. \tag{4.2}$$

Let us now carefully consider the simple continued fraction expansion to $\sqrt[3]{a} = \sqrt[3]{x^3-1}$. As a routine exercise in calculus, we have, provided $x \geqslant 3$, partial quotients $a_i$ given by

$$a_0 = x - 1, \qquad a_1 = 1, \qquad a_2 = 3x^2 - 2, \qquad a_3 = 1,$$
$$a_4 = x - 2 \quad \text{and} \quad a_5 = 1.$$

From (4.2) and the fact that $j$ is even, it follows, for $x \geqslant 3$, that $j \geqslant 6$.

For $x \neq 2, 3, 5, 7$, we further have

$$a_6 = \begin{cases} (9x^2-4)/2 & \text{if } x \equiv 0 \pmod 2, \\ (9x^2-3)/2 & \text{if } x \equiv 1 \pmod 2, \end{cases}$$

$$a_7 = \begin{cases} 1 & \text{if } x \equiv 0 \pmod 2, \\ 2 & \text{if } x \equiv 1 \pmod 2 \end{cases}$$

and

$$a_8 = \begin{cases} (4x-10)/5 & \text{if } x \equiv 0 \pmod{10}, \\ (x-6)/5 & \text{if } x \equiv 1 \pmod{10}, \\ (4x-8)/5 & \text{if } x \equiv 2 \pmod{10}, \\ (x-3)/5 & \text{if } x \equiv 3 \pmod{10}, \\ (4x-6)/5 & \text{if } x \equiv 4 \pmod{10}, \\ (x-5)/5 & \text{if } x \equiv 5 \pmod{10}, \\ (4x-9)/5 & \text{if } x \equiv 6 \pmod{10}, \\ (x-7)/5 & \text{if } x \equiv 7 \pmod{10}, \\ (4x-7)/5 & \text{if } x \equiv 8 \pmod{10}, \\ (x-4)/5 & \text{if } x \equiv 9 \pmod{10}. \end{cases}$$

From inequality (4.2), we conclude (except, possibly, for $x \in \{2, 3, 5, 7\}$) that $z/y = p_j/q_j$ with $j \geqslant 8$. We calculate that

$$q_8 = \begin{cases} (108x^6 - 135x^5 - 90x^3 + 75x^2 + 10)/10 & \text{if } x \equiv 0 \pmod{10}, \\ (54x^6 - 189x^5 - 45x^3 + 105x^2 + 5)/10 & \text{if } x \equiv 1 \pmod{10}, \\ (108x^6 - 81x^5 - 90x^3 + 45x^2 + 10)/10 & \text{if } x \equiv 2 \pmod{10}, \\ (54x^6 - 27x^5 - 45x^3 + 15x^2 + 5)/10 & \text{if } x \equiv 3 \pmod{10}, \\ (108x^6 - 27x^5 - 90x^3 + 15x^2 + 10)/10 & \text{if } x \equiv 4 \pmod{10}, \\ (54x^6 - 135x^5 - 45x^3 + 75x^2 + 5)/10 & \text{if } x \equiv 5 \pmod{10}, \\ (54x^6 - 54x^5 - 45x^3 + 30x^2 + 5)/5 & \text{if } x \equiv 6 \pmod{10}, \\ (54x^6 - 243x^5 - 45x^3 + 135x^2 + 5)/10 & \text{if } x \equiv 7 \pmod{10}, \\ (54x^6 - 27x^5 - 45x^3 + 15x^2 + 5)/5 & \text{if } x \equiv 8 \pmod{10}, \\ (54x^6 - 81x^5 - 45x^3 + 45x^2 + 5)/10 & \text{if } x \equiv 9 \pmod{10}, \end{cases}$$

and so

$$y \geqslant q_8 > 5x^6,$$

except, possibly, for

$$x \in \{2, 3, 5, 7, 9, 11, 15, 17, 19, 21, 25, 27, 31, 37, 41, 47, 57\}.$$

For the values in this set with $x \geqslant 9$, direct computation gives that $a_9 \leqslant 10$ (with equality for those $x \equiv 3 \pmod{10}$) and hence the first inequality in (4.2) ensures that

$$y \geqslant q_{10} > 5x^6.$$

For $x \in \{2, 3, 5, 7\}$, computing the continued fraction expansions to $\sqrt[3]{x^3 - 1}$, we find that the corresponding convergents $p_j/q_j$ with $q_j \leqslant 5x^6$ and $j$ even all satisfy $j \leqslant 6$. A short calculation reveals that

$$(x^3 - 1) \cdot q_j^3 - p_j^3 \quad \text{divides} \quad x^3 - 2$$

only for $x = 2$ and $j = 0$ (whereby $z = y$, an immediate contradiction).

It follows, then, for all $x \geqslant 2$, we may assume that $y > 5x^6$ and so

$$b > 125a^6. \tag{4.3}$$

Combining this inequality with (2.13), we find, for $x \geqslant 4$, that

$$a^{15-7\lambda} < 2^9 \cdot 3^{3/2} \cdot 5^{9-3\lambda},$$

with

$$\lambda = 1 + \frac{\log(3\sqrt{3}(\sqrt{a} + \sqrt{a+1})^2)}{\log(\frac{1}{3\sqrt{3}}(\sqrt{a} + \sqrt{a+1})^2)}.$$

Since $a = x^3 - 1$, this inequality is a contradiction as soon as $x \geqslant 7973$.

It remains to treat $2 \leqslant x \leqslant 7972$. If $4 \leqslant x \leqslant 7972$, we have

$$z < \left(8\sqrt{3}a^2\right)^{1/(3-\lambda)} < 10^{32}.$$

For each of these values of $x$, we again compute the initial terms in the infinite simple continued fraction expansions to $\sqrt[3]{x^3 - 1}$, verifying that for each convergent $p_j/q_j$ with $p_j < 10^{32}$ and $q_j > 1$, $(x^3 - 1) \cdot q_j^3 - p_j^3$ fails to divide $x^3 - 2$.

For the remaining values $x \in \{2, 3\}$, we appeal to Corollary 1.2 of [3], where we find that

$$\left|\sqrt[3]{7} - \frac{p}{q}\right| > \frac{0.08}{q^{2.70}}, \quad \text{and} \quad \left|\sqrt[3]{26} - \frac{p}{q}\right| > \frac{0.03}{q^{2.53}},$$

valid for all positive integers $p$ and $q$. Combining these with (4.1), we find that $y \leqslant 852$ (if $x = 2$) and $y \leqslant 1646$ (if $x = 3$). A short check reveals that no such choices of $y > 1$ satisfy (1.3). This completes the proof of Theorem 1.1, in case $x$, $y$ and $z$ are positive integers.

## 5. THE CASES WHERE $x = -1$ IN THEOREMS 1.1 AND 1.2

Before we proceed with the remainder of our proof (corresponding to having $\min\{x, y, z\}$ negative in Theorems 1.1, and to Theorem 1.2), we note that the case where, say, $x = -1$ is a special one. In particular, it is the only situation where we cannot ensure that each of $x^k - 1$, $y^k - 1$ and $z^k - 1$ grows (in absolute value, at least) exponentially in $k$. As may be noted from the preceding sections, this is used crucially in our application of techniques from Diophantine approximation.

The case where one of $x$ or $y$ is equal to $-1$ in Theorem 1.2 (say $x = -1$) is, in fact, easily treated. If such a solution exists, then there necessarily exists an integer $m$ such that

$$y^k + 1 = 2m^2.$$

Since $k \geqslant 5$, a result of the author with Chris Skinner (Proposition 8.1 of [7]) implies that $y = 1$ (contradicting $y \neq \pm x$).

We now proceed with the proof of Theorem 1.1 with $x = -1$. Taking $x = -1$ in equation (1.3) (assuming that $k$ is odd), we find that necessarily $z^k - 2y^k = 3$. This is a *binomial Thue equation.* A straightforward application of lower bounds for linear forms in two (complex) logarithms of algebraic numbers to, given the more general situation of finding all solutions with $|XY| > 1$ to an equation of the form $AX^k - BY^k = C$, explicitly bounds $k$, solely in terms of $A$, $B$ and $C$. The tricky part of solving such equations, then, lies in handling "small" (but not too small) values of $k$. Generally, if $A \pm B \neq C$, we may treat such equations via Frey curves (see e.g. [6]).

For our purposes, we will appeal to the following

**Proposition 5.1.** *The only solutions to the Diophantine inequality*

$$|X^k - 2Y^k| \leqslant 100 \tag{5.1}$$

*in coprime, positive integers $X, Y$ and $k \geqslant 3$ satisfy $Y^k < 1000$ or*

$$(X, Y, k) \in \{(14, 11, 3), (29, 23, 3), (34, 27, 3), (63, 50, 3), (6, 5, 4)\}.$$

*In particular, the only solutions to the equation*

$$X^k - 2Y^k = 3 \tag{5.2}$$

*in integers $X, Y$ and $k \geqslant 3$ are given by $(X, Y, k) = (1, -1, k)$ for $k$ odd, and by $(X, Y, k) = (-5, -4, 3)$.*

**Proof.** There are many different ways to attack such binomial Thue equations of arbitrary degree, based upon, for instance, a reasonably flexible version of the hypergeometric method of Thue and Siegel [5], or upon Frey curves à la Wiles, perhaps in conjunction with lower bounds for linear forms in logarithms (see e.g. [6]). We will employ both of these approaches in our proof.

Let us note that the desired result is essentially a sharpening of work of Györy and Pintér (Theorem 4 of [16]), who solved equation (5.2) for all values of $k$ except

$$k \in \{19, 23, 29, 31, 37, 41, 43, 47, 73\}. \tag{5.3}$$

Arguing as in that paper, a routine application of lower bounds for linear forms in two complex logarithms (such as those leading to [19]), together with computation of initial convergents in the continued fraction expansions to $\sqrt[k]{2}$ for $k \leqslant 600$ or

so, provides the conclusion that, if there are additional solutions to inequality (5.1), necessarily $k \leqslant 350$. We may assume, without loss of generality, that $k$ is an odd prime, or that $k = 4$.

We begin by supposing $k = 3$. In this situation, we will use the inequality

$$|X^3 - 2Y^3| \geqslant \sqrt{X},$$

valid for positive integers $X$ and $Y$ (see [3]). This implies that integers $(X, Y)$ satisfying inequality (5.1) necessarily have $|X| \leqslant 10^4$. A quick search reveals the stated solutions.

For $k = 4$ or $5 \leqslant k < 350$ prime, we search for local obstructions to the equation

$$X^k - 2Y^k = m, \tag{5.4}$$

where $|m| \leqslant 100$. If $k = 4$, for instance, we consider this equation modulo 5, 13, 16 and 17 to conclude that

$$m \in \{-97, -82, -79, -49, -31, -2, -1, 1, 14, 46, 49, 79, 94\}.$$

Explicitly solving these remaining Thue equations via Pari uncovers only "small" solutions as noted in the statement of Proposition 5.1. The algorithm in Pari to solve such equations relies upon lower bounds for linear forms in complex logarithms, together with the Lenstra–Lenstra–Lovacz lattice basis reduction algorithm. For $k > 4$, we appeal to work of Darmon and Merel [13] and Ribet [21] to conclude that (5.4) has no solutions with $\max\{|X|, |Y|\} > 1$, provided $|m| \leqslant 2$.

For odd values of $k$, it is no loss of generality to assume that $m$ is positive (and not divisible by 4) in equation (5.4). In case $k = 5$ or $k = 7$, we argue similarly to the case $k = 4$, dealing with equation (5.4) for

$$m \equiv 0, \pm 1, \pm 2, \pm 3 \pmod{11}, \qquad m \not\equiv 0 \pmod{4}$$

and

$$m \in \{3, 7, 14, 15, 19, 22\text{–}25, 29, 34, 35, 39, 43, 46, 51, 54\text{–}57, 61, 62, 73, 75, 81\text{–}94, 97, 99\},$$

respectively, again via Pari.

For $11 \leqslant k < 350$ prime, we will split our argument into two parts, depending on whether $m = 3$ or $m > 3$.

### 5.1. The case $m > 3$

If $m > 3$, then local arguments (considering equation (5.4) modulo $q$ for various $q$, typically primes $q \equiv 1 \pmod{k}$) eliminate all cases of (5.4), except for

$$\begin{aligned} k = 11: &\quad m \in \{21, 22, 66, 67, 70\}, \\ k = 13: &\quad m \in \{23, 25, 45, 46, 55, 69, 78\}, \\ k = 17: &\quad m = 55, \\ k = 19: &\quad m \in \{37, 53, 71, 79, 94, 95, 97\}, \end{aligned}$$

and $k = 23$, $m = 45$. The largest prime we need consider to find a local obstruction is $q = 9511$, for $k = 317$ and $m \in \{19, 43, 45, 98\}$. For these remaining cases of (5.4) with $m > 3$, we will use arguments that depend crucially on the modularity of Galois representations associated to certain elliptic curves; as far as the author is aware, these were first applied in the setting of binomial Thue equations in [6]. Specifically, supposing we have an integral solution to (5.4), we consider one of the following (Frey or Frey–Hellegouarch) curves:

$$\begin{aligned} E_1&: y^2 = x(x+m)\big(x - 2Y^k\big), \quad \text{if } m \equiv 1 \pmod{4}, \\ E_2&: y^2 = x(x-m)\big(x + 2Y^k\big), \quad \text{if } m \equiv -1 \pmod{4}, \\ E_3&: y^2 = x(x+m/2)\big(x + X^k/2\big), \quad \text{if } m \equiv 2 \pmod{8}, \end{aligned}$$

and

$$E_4: y^2 = x(x - m/2)(x - X^k/2), \quad \text{if } m \equiv -2 \pmod{8}.$$

Let us define, for $l$ a prime of good reduction of $E_i$,

$$a_l(E_i) = l + 1 - \big|E(\mathbb{F}_l)\big|$$

and

$$N_1 = N_2 = \begin{cases} 2\,\mathrm{rad}(m) & \text{if } Y \text{ is even}, \\ 32\,\mathrm{rad}(m) & \text{if } Y \text{ is odd}, \end{cases}$$
$$N_3 = N_4 = \mathrm{rad}(m),$$

where $\mathrm{rad}(m)$ denotes the product of the distinct primes dividing $m$. By now-standard arguments (see e.g. [8,10,17]), there exists a weight 2 cuspidal newform of level $N_i$,

$$f = \sum_{j=1}^{\infty} c_j q^j, \quad c_j \in F$$

and a prime ideal $\mathbf{k}$ of $F$, lying above $k$, such that, for each prime $l$ coprime to $2km$, we have either

$$a_l(E_i) \equiv c_l \pmod{\mathbf{k}} \tag{5.5}$$

or

$$\pm(l+1) \equiv c_l \pmod{\mathbf{k}}, \tag{5.6}$$

depending on whether $E_i$ has good or multiplicative reduction at $l$. As noted in [10] (see Lemma 2.1), we may be rather more precise in the case where $F = \mathbb{Q}$.

As it transpires, these congruences suffice to eliminate each newform at the levels $N_i$ under consideration, for the Frey curves corresponding to the remaining 21 equations of the shape (5.4). We will describe our argument in full for the equation

$$X^{17} - 2Y^{17} = 55, \tag{5.7}$$

which exhibits all features of interest; we suppress the details for the other equations. We note that computation of the newforms in question may be carried out via Magma or one may consult William Stein's Modular Forms Database.

From the preceding discussion, a solution in integers $(X, Y)$ to (5.7) corresponds via the curve $E_2$ to a newform of level $N_2 = 110$ or 1760, depending as $Y$ is even or odd. For each newform of level 110, both (5.5) or (5.6) lead to contradictions for $l = 3$. At level 1760, we reach like conclusions using one of $l = 3, 7$ or 13, for every newform except a pair of one-dimensional forms (i.e. with $F = \mathbb{Q}$) corresponding to the elliptic curves over $\mathbb{Q}$ given as 1760f and 1760j in Cremona's tables:

$$y^2 = x^3 - 37x + 84 \quad \text{and} \quad y^2 = x^3 - 37x - 84.$$

Noting that, from (5.7), we necessarily have

$$Y^{17} \equiv -1 \pmod{307}$$

and so

$$a_{307}(E_2) = -12.$$

Since the curves 1760f and 1760j have Fourier coefficient $c_{307} = \pm 4$, this contradicts (5.5).

As a final comment in the case $m > 3$, let us note the interesting example

$$X^{19} - 2Y^{19} = 37,$$

with $Y$ even. Here we are led to consider weight 2 newforms at level 74, where there lurks a form $f$ for which (5.6) is satisfied for *every* large prime $l$ ($f$ is congruent modulo 19 to an Eisenstein series). To eliminate the possibility of this form "giving rise" to our Frey curve ($E_1$ in this case), we may either appeal to the arguments leading to Lemma 7.1 of [10], or note that $a_{191}(E_1) = 16$, contradicting (5.6).

### 5.2. The case $m = 3$

To complete the proof of Proposition 5.1, it remains to handle equation (5.4) with $m = 3$. As noted earlier, we may suppose $k$ satisfies (5.3). For $19 \leqslant k \leqslant 31$, we, as previously, solve (5.4) via Pari. These are substantial calculations, since we wish to avoid dependence upon the generalized Riemann hypothesis to obtain unconditional results. At the present time, these are not far from as large a Thue solving problem as one might reasonably tackle via Pari.

For the remaining values of $k$, we will turn to a result derived from the hypergeometric method of Thue and Siegel:

**Theorem 5.2.** *Let $b > a$ be positive, relatively prime integers, suppose that*

$$37 \leqslant n \leqslant 73 \quad \textit{is prime,} \qquad m = \left[\frac{n+1}{3}\right],$$

*and define $c(n)$ via*

| $n$ | $c(n)$ | $n$ | $c(n)$ |
|---|---|---|---|
| 37 | 21.2 | 59 | 38.5 |
| 41 | 25.2 | 61 | 39 |
| 43 | 26 | 67 | 44 |
| 47 | 30 | 71 | 48 |
| 53 | 34 | 73 | 52 |

*If we have*

$$\left(\sqrt[m]{b} - \sqrt[m]{a}\right)^m e^{c(n)} < 1,$$

*then, if $p$ and $q > 0$ are integers, we may conclude that*

$$\left|\left(\frac{b}{a}\right)^{1/n} - \frac{p}{q}\right| > \left(5 \times 10^{75}\left(\sqrt[m]{b} + \sqrt[m]{a}\right)^m\right)^{-1} q^{-\lambda},$$

*where*

$$\lambda = (m-1)\left\{1 - \frac{\log((\sqrt[m]{b} + \sqrt[m]{a})^m e^{c(n)+1/20})}{\log((\sqrt[m]{b} - \sqrt[m]{a})^m e^{c(n)})}\right\}.$$

This result is a small sharpening of certain cases of Theorem 7.1 of [5], to enable us, upon choosing $a = 2$, $b = 1$, to deduce explicit improvements upon Liouville's Theorem for $\sqrt[k]{2}$ for $37 \leqslant k \leqslant 73$ prime. These new estimates arise from a straightforward appeal to recent computations of Rubinstein, who found the 100,000 smallest zeros of each Dirichlet $L$-function with conductor $p < 50$ and the first 10,000 zeros for each Dirichlet $L$-function with conductor $p < 100$, greatly

improving the corresponding results in [5]. For details of how this information may be applied to deduce results like Theorem 5.2, we direct the reader to [5] and [20].

Since the equality $|x^k - 2y^k| = 3$ implies the inequality

$$\left|\sqrt[k]{2} - \frac{x}{y}\right| < \frac{3}{k|y|^k},$$

we have, applying Theorem 5.2, for prime $k$ with $37 \leqslant k \leqslant 73$, that $|y| < 10^{3600}$. The usual continued fraction search up to this bound, reveals no solutions with $|y| > 1$. □

## 6. SOME NECESSARY MODIFICATIONS

To complete the proofs of Theorems 1.1 and 1.2, we need to treat equations (1.4), (2.1), (2.2), (2.3), (2.4) and (2.5), in positive integers $x, y, z$ and $k \geqslant 3$ prime. Our argument is much as in the preceding sections; solutions to these equations imply the existence of positive integers $a, b$ and $c$ for which

$$(6.1) \qquad a-1=x^k, \qquad b-1=y^k, \qquad ab+1=z^k,$$

$$(6.2) \qquad a-1=x^k, \qquad b+1=y^k, \qquad ab-1=z^k,$$

$$(6.3) \qquad ab^2+1=x^k, \qquad ac^2+1=y^k, \qquad abc+1=z^k,$$

$$(6.4) \qquad ab^2+1=x^k, \qquad ac^2+1=y^k, \qquad abc-1=z^k,$$

$$(6.5) \qquad ab^2-1=x^k, \qquad ac^2-1=y^k, \qquad abc+1=z^k$$

or

$$(6.6) \qquad ab^2-1=x^k, \qquad ac^2-1=y^k, \qquad abc-1=z^k,$$

respectively. In the first case, we may assume that $b > a$. In the second, we need treat the cases $a < b$ and $a > b$ separately. For the final four cases, we may suppose that $c > b$.

### 6.1. Gap principles

For cases (6.1) and (6.2), the modifications to our earlier work are rather minor. For (6.3), (6.4), (6.5) and (6.6), they are less so; we illustrate this in case (6.3).

From (6.3), we may suppose that $xy = z^2 + t$ for $t \in \mathbb{N}$ and so, assuming $c > b$, in analogy to (2.7),

$$(6.7) \qquad c > (kt)^{k/2} a^{(k-2)/2} b^{k-1}.$$

Again appealing to (6.3),

$$\left(1 + \frac{1}{ab^2}\right) - \left(\frac{xy}{z^2}\right)^k = \frac{2a^2b^3c - a^2b^4 + 2abc + 1}{a^3b^4c^2 + 2a^2b^3c + ab^2}.$$

Thus

$$0 < \sqrt[k]{1+\frac{1}{ab^2}} - \frac{xy}{z^2} < \frac{2.1}{kabc}.$$

Our previous arguments, together with the gap principle (6.7) lead to a contradiction, provided $k \geqslant 5$. We notice that this inequality, in the case $k = 3$, does not imply that $xy/z^2$ is even a convergent in the continued fraction expansion to $\sqrt[k]{1+\frac{1}{ab^2}}$, let alone an exceedingly "good" one (information which underlies our proofs in the other cases). It is for this reason that we are unable to extend Theorem 1.2 to include $k = 3$.

### 6.2. $k = 4$ in Theorem 1.2

The final case in our proofs to treat is that of $k = 4$ in Theorem 1.2, which we must, by necessity, handle somewhat differently. If we have

$$(x^4 - 1)(y^4 - 1) = (z^4 - 1)^2,$$

then we may write $x^4 - 1 = ab^2$ and $y^4 - 1 = ac^2$, where $b$ and $c$ are distinct positive integers (so, in particular, $a$ is a nonsquare positive integer). It follows from a theorem of Cohn [11] that $x = 13$ and $y = 239$. Since 9653280 is not of the form $z^4 - 1$, we conclude as stated.

## 7. THE EQUATION $(x^3 - 1)(y^3 - 1) = (z^3 - 1)^2$

As noted earlier, we are unable to say anything of substance regarding equation (1.4) in case $k = 3$. In point of fact, the more general equation

$$(x^3 - 1)(y^3 - 1) = u^2$$

quite likely has only finitely many solutions in integers $(x, y, u)$ with $u$ positive and $x \neq y$. Noam Elkies, at the instigation of Gary Walsh, ran a short computation to unearth the solutions

$$(x, y, u) = (-20, -362, 616077), (-6, -26, 1953), (-1, -23, 156), (0, -2, 3),$$
$$(2, 4, 21), (2, 22, 273), (3, 313, 28236), (4, 22, 819).$$

Perhaps there are no others.

## REFERENCES


[1] Baker A. – Rational approximations to certain algebraic numbers, Proc. London Math. Soc. **14** (3) (1964) 385–398.

[2] Baker A. – Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, Quart. J. Math. Oxford Ser. (2) **15** (1964) 375–383.

[3] Bennett M.A. – Effective measures of irrationality for certain algebraic numbers, J. Austral. Math. Soc. **62** (1997) 329–344.

[4] Bennett M.A. – Explicit lower bounds for rational approximation to algebraic numbers, Proc. London Math. Soc. **75** (1997) 63–78.

[5] Bennett M.A. – Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$, J. Reine Angew. Math. **535** (2001) 1–49.

[6] Bennett M.A. – Products of consecutive integers, Bull. London Math. Soc. **36** (2004) 683–694.

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

[8] Bennett M.A., Győry K., Mignotte M., Pínter A. – Binomial Thue equations and polynomial powers, Compositio Math. **142** (2006) 1103–1121.

[9] Bugeaud Y. – On the Diophantine equation $(x^k - 1)(y^k - 1) = (z^k - 1)$, Indag. Mathem. **15** (2004) 21–28.

[10] Bugeaud Y., Mignotte M., Siksek S. – A multi-Frey approach to some multi-parameter families of Diophantine equations, Canad. J. Math., to appear.

[11] Cohn J.H.E. – The Diophantine equation $x^4 - Dy^2 = 1$. II, Acta Arith. **78** (1997) 401–403.

[12] Darmon H., Granville A. – On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$, Bull. London Math. Soc. **27** (1995) 513–544.

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

[14] Dujella A. – There are only finitely many Diophantine quintuples, J. Reine Angew. Math. **566** (2004) 183–214.

[15] Guy R.K. – Unsolved Problems in Number Theory, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004, xviii+437 pp.

[16] Győry K., Pintér A. – Almost perfect powers in products of consecutive integers, Monatsh. Math. **145** (2005) 19–33.

[17] Kraus A. – Majorations effectives pour l'équation de Fermat généralisée, Canad. J. Math. **49** (6) (1997) 1139–1161.

[18] Leveque W.J. – Topic in Number Theory, Addison-Wesley, Reading, 1956.

[19] Mignotte M. – A note on the equation $ax^n - by^n = c$, Acta Arith. **75** (1996) 287–295.

[20] Ramaré O., Rumely R. – Primes in arithmetic progressions, Math. Comp. **65** (1996) 397–425.

[21] Ribet K. – On the equation $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. **79** (1997) 7–16.

[22] Szymiczek K. – The equation $(x^2 - 1)(y^2 - 1) = (z^2 - 1)^2$, Eureka **35** (1972) 21–25.

[23] Thue A. – Berechnung aller Lösungen gewisser Gleichungen von der form, Vid. Skrifter I. Mat.-Naturv. Klasse (1918) 1–9.

(Received 19 August 2006)