

# ON A THEOREM OF TARTAKOWSKY

MICHAEL A. BENNETT

*Dedicated to the memory of Béla Brindza*

ABSTRACT. Binomial Thue equations of the shape  $Aa^n - Bb^n = 1$  possess, for  $A$  and  $B$  positive integers and  $n \geq 3$ , at most a single solution in positive integers  $a$  and  $b$ . In case  $n \geq 4$  is even and  $A = 1$ , an old result of Tartakowsky characterizes this solution, should it exist, in terms of the fundamental unit in  $\mathbb{Q}(\sqrt{B})$ . In this note, we extend this to certain values of  $A > 1$ .

## 1. INTRODUCTION

If  $F(x, y)$  is an irreducible binary form of degree  $n \geq 3$ , then the *Thue* equation

$$F(x, y) = m$$

has, for a fixed nonzero integer  $m$ , at most finitely many solutions which may, via a variety of techniques from the theory of Diophantine approximation, be effectively determined (see e.g. Tzanakis and de Weger [14]). In general, the number of such solutions may depend upon the degree of  $F$ , but, as proven by Mueller and Schmidt [10], is bounded solely in terms of  $m$  and the number of monomials of  $F$ . In the special case where  $m \leq 2$  and the number of monomials is minimal, we have the following recent theorem of the author's :

**Theorem 1.1.** ([2]) *If  $A, B$  and  $n$  are nonzero integers with  $n \geq 3$ , then the inequality*

$$|Aa^n - Bb^n| \leq 2$$

*has at most one solution in positive integers  $(a, b)$ .*

In particular, an equation of the form

$$(1.1) \quad Aa^n - Bb^n = 1$$

has, for fixed  $AB \neq 0$  and  $n \geq 3$ , at most a single positive solution  $(a, b)$  (this is, in fact, the main result of [1]). This statement, while in some sense sharp, fails to precisely characterize the solutions that occur. Given the existence of a pair of integers  $(a, b)$  satisfying (1.1), for instance, it would be of some interest to determine their relationship with the structure of  $\mathbb{Q}(\sqrt[n]{B/A})$ , in particular with the fundamental unit(s) in the ring of integers of this field. A prototype of the result we have in mind is the following special case of a theorem of Ljunggren [9] (cf. Nagell [11]) :

---

1991 *Mathematics Subject Classification.* Primary 11D41, Secondary 11D45, 11B37.  
*Key words and phrases.* Thue equations, Frey curves.  
Supported in part by a grant from NSERC.

**Theorem 1.2.** (*Ljunggren*) *If  $A$  and  $B$  are positive integers, then if  $a$  and  $b$  are positive integers for which*

$$Aa^3 - Bb^3 = 1,$$

*we necessarily have that*

$$\left(a\sqrt[3]{A} - b\sqrt[3]{B}\right)^3$$

*is either the fundamental unit or its square in the field  $\mathbb{Q}(\sqrt[3]{A/B})$ .*

For larger (even) values of  $n$ , where, additionally, we assume that  $A = 1$ , we have a result stated by Tartakowsky [13] and proved by Af Ekenstam [6] :

**Theorem 1.3.** (*Tartakowsky, Af Ekenstam*) *Let  $n$  and  $B$  be integers with  $n \geq 2$ ,  $B$  positive and nonsquare and  $(n, B) \neq (2, 7140)$ . If there exist positive integers  $a$  and  $b$  such that*

$$(1.2) \quad a^{2n} - Bb^{2n} = 1,$$

*then*

$$u_1 = a^n \quad \text{and} \quad v_1 = b^n.$$

*If  $(n, B) = (2, 7140)$ , then equation (1.2) has precisely one solution in positive integers, corresponding to*

$$u_2 = 239^2 \quad \text{and} \quad v_2 = 26^2.$$

Here and subsequently, we define  $u_1$  and  $v_1$  to be the smallest positive integers such that  $u_1^2 - Bv_1^2 = 1$  and set

$$u_k + v_k\sqrt{B} = (u_1 + v_1\sqrt{B})^k.$$

Our goal in this paper is to consider the more general equation

$$(1.3) \quad M^2 a^{2n} - Bb^{2n} = 1.$$

In case  $M = 2^{n-1}$ , an analogous result to Theorem 1.3 is noted without proof by Ljunggren (as Theorem II of [8]). In [3], this is generalized to  $M = 2^\alpha$  for arbitrary nonnegative integer  $\alpha$ . Here, we extend this result to (certain) larger values of  $M$ . Specifically, defining  $P(M)$  to be the largest prime divisor of  $M$ , we prove

**Theorem 1.4.** *Let  $M, n$  and  $B$  be positive integers with  $M, n \geq 2$ ,  $B$  nonsquare and  $P(M) \leq 13$ . If there exist positive integers  $a$  and  $b$  satisfying (1.3) then either  $u_1 = Ma^n$  and  $v_1 = b^n$ , or one of  $(M, n, B) = (1, 2, 7140)$  or  $(7, 2, 3)$ . In these latter cases, we have  $u_2 = Ma^n$  and  $v_2 = b^n$ .*

## 2. THE CASE $n = 2$

We begin our proof of Theorem 1.4 by treating the case  $n = 2$ . Here, we will deduce something a bit stronger, generalizing Corollary 1.3 of [5] in the process :

**Proposition 2.1.** *Let  $M, B > 1$  be squarefree integers with  $P(M) \leq 13$ . Then if there exist positive integers  $a$  and  $c$  satisfying the Diophantine equation*

$$(2.1) \quad M^2 a^4 - Bc^2 = 1,$$

*we necessarily have  $Ma^2 = u_k$  with  $k = 1$  unless either  $M = 7$  (in which case  $k = 1$  or  $k = 2$ , but not both) or*

$$(2.2) \quad (M, B) \in \{(11, 2), (26, 3), (26, 16383), (55, 1139), (1001, 571535)\},$$

*where we have  $k = 3$ .*

The aforementioned Corollary 1.3 of [5] is just the above result under the more restrictive assumption  $P(M) \leq 11$ . We will thus assume for the remainder of this section that  $13 \mid M$ . Our argument is similar to that given in [5]; we will suppress many of the details.

From Theorem 1.2 and Lemma 5.1 of [5], we have  $Ma^2 = u_k$  with  $k$  a positive integral divisor of 420. Since  $u_{2j} = 2u_j^2 - 1$  and  $13 \mid M$ , we may suppose that  $k$  is odd. Now, by the classical theory of Pell's equation, we have that

$$u_k = T_k(u_1),$$

where  $T_k(x)$  denotes the  $k$ th Tschebyscheff polynomial (of the first kind), satisfying

$$T_k(x) = \cos(k \arccos x) = x^k + \binom{k}{2} x^{k-2}(x^2 - 1) + \dots$$

for  $k$  a nonnegative integer. Since  $T_{k_1 k_2}(x) = T_{k_1}(T_{k_2}(x))$  for positive integers  $k_1$  and  $k_2$ , to conclude as desired, we need only solve the Diophantine equations

$$(2.3) \quad T_k(x) = Ma^2, \quad k \in \{3, 5, 7\}$$

in integers  $x$  and  $a$  with  $x > 1$ . If  $k = 5$  or  $k = 7$ , we note that  $T_k(x) = x(16x^4 - 20x^2 + 5)$  or  $x(64x^6 - 112x^4 + 56x^2 - 7)$ , respectively. Since

$$\gcd(16x^4 - 20x^2 + 5, 2 \cdot 3 \cdot 7 \cdot 11 \cdot 13) = 1,$$

in the first case, from (2.3), we necessarily have

$$16x^4 - 20x^2 + 5 = 5^\delta u^2$$

for some  $u \in \mathbb{Z}$  and  $\delta \in \{0, 1\}$ . Arguing as in the proof of Corollary 1.3 of [5] leads to a contradiction if  $x > 1$ . In case  $k = 7$ , since

$$\gcd(64x^6 - 112x^4 + 56x^2 - 7, 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13) = 1,$$

it follows that

$$64x^6 - 112x^4 + 56x^2 - 7 = 7^\delta u^2,$$

again for  $u \in \mathbb{Z}$  and  $\delta \in \{0, 1\}$ . From the inequalities

$$(8x^3 - 7x)^2 < 64x^6 - 112x^4 + 56x^2 - 7 < (8x^3 - 7x + 1)^2$$

valid for  $x > 1$ , we may suppose that  $\delta = 1$  (so that  $7 \mid x$ ). It follows that  $7 \mid u^2 + 1$ , again a contradiction.

Finally, if  $k = 3$ , we are left to consider equations of the form

$$x(4x^2 - 3) = Ma^2, \quad P(M) \leq 13.$$

Via (nowadays) routine computations using linear forms in elliptic logarithms and lattice basis reduction (as implemented, for example, in Simath), we find that the only solutions to these equations with  $x > 1$  correspond to

$$x \in \{2, 3, 128, 135, 756\}.$$

This, after a simple calculation, completes the proof of Proposition 2.1.

To apply this to Theorem 1.4 in case  $n = 2$ , let us begin by supposing that there exist positive integers  $a$  and  $b$  such that

$$(2.4) \quad M^2 a^4 - B b^4 = 1.$$

Writing  $B = B_0 B_1^2$  with  $B_0$  squarefree, we will, as previously, take  $u_1$  and  $v_1$  for the smallest positive integers with  $u_1^2 - B v_1^2 = 1$  and suppose that  $u_1^*$  and  $v_1^*$  are the smallest positive integers satisfying  $(u_1^*)^2 - B_0 (v_1^*)^2 = 1$ . From Proposition 2.1,

it follows that  $Ma^2 = u_k^*$  and  $B_1b^2 = v_k^*$  for  $k \leq 3$ . Since  $u_k^* \leq u_k$  for all  $k$ , it remains to show that  $k = 1$ . If  $k = 3$ , from (2.2),

$$Ma^2 \in \{26, 99, 8388224, 9841095, 1728322596\}.$$

In each case, we find that  $M^2a^4 - 1$  is fourth-power free, except if  $Ma^2 = 9841095$  where  $16 \mid M^2a^4 - 1$ . It follows that either  $B$  or  $16B$  is equal to  $M^2a^4 - 1$ , contradicting, in every case,  $k > 1$ .

If  $k = 2$ , then, from Proposition 2.1, we have  $M = 7$  and hence

$$7a^2 = u_2^* = 2(u_1^*)^2 - 1, \quad B_1b^2 = v_2^* = 2u_1^*v_1^*.$$

If  $u_1^* < u_1$  then necessarily  $7a^2 = u_1$ , as desired. We may thus suppose that  $u_1 = u_1^*$  and hence that  $u_1^*$  is coprime to  $B_1$ . From the first of the above two equations, we may conclude that  $u_1^*$  is even whereby, from the second,  $u_1^* = 2r^2$  for some integer  $r$ . The first equation then implies that

$$8r^4 - 7a^2 = 1$$

whence, from Proposition 2.1,  $|ar| = 1$ . We thus have  $Bb^4 = 48$ , as claimed.

### 3. LARGER VALUES OF $n$

Let us now suppose that  $n \geq 3$  is prime. Let  $\epsilon = u + v\sqrt{B}$  where  $u$  and  $v$  are positive integers (to be chosen later) with  $u^2 - Bv^2 = 1$ . Defining

$$E_k = \frac{\epsilon^k - \epsilon^{-k}}{\epsilon - \epsilon^{-1}},$$

if  $p$  is an odd positive integer, then we have the following identities :

$$(3.1) \quad \left(E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}}\right) \left(E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}}\right) = E_p$$

$$(3.2) \quad (u+1) \left(E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}}\right)^2 - (u-1) \left(E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}}\right)^2 = 2$$

$$(3.3) \quad (u+1) \left(E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}}\right)^2 + (u-1) \left(E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}}\right)^2 = \epsilon^p + \epsilon^{-p}.$$

If we suppose that there exist positive integers  $a$  and  $b$  with  $M^2a^{2n} - Bb^{2n} = 1$ , we may write

$$(3.4) \quad Ma^n + b^n\sqrt{B} = (u_1 + v_1\sqrt{B})^m$$

for some positive integer  $m$ . We separate our proof into two cases, depending on whether or not  $m$  has an odd prime divisor  $p$ . If such a prime  $p$  exists, define

$$\epsilon = a_1 + b_1\sqrt{B} = (u_1 + v_1\sqrt{B})^{m/p},$$

so that

$$(3.5) \quad Ma^n + b^n\sqrt{B} = (a_1 + b_1\sqrt{B})^p.$$

Expanding via the binomial theorem and equating coefficients, we thus may write

$$Ma^n = a_1 \cdot a_2, \quad b^n = b_1 \cdot b_2$$

where  $a_2$  and  $b_2$  are odd integers with

$$\gcd(a_1, a_2), \gcd(b_1, b_2) \in \{1, p\}$$

and neither  $a_2$  nor  $b_2$  divisible by  $p^2$ . It follows that there exists a positive integer  $s$  such that either  $b_1 = s^n$  or  $b_1 = p^{n-1}s^n$ . In the first case,  $E_p = (b/s)^n$  and so, from (3.1) and the fact that the two factors on the left hand side of (3.1) are coprime,

$$E_{\frac{p+1}{2}} - E_{\frac{p-1}{2}} = P^n \quad \text{and} \quad E_{\frac{p+1}{2}} + E_{\frac{p-1}{2}} = Q^n,$$

for some positive integers  $P$  and  $Q$ . Equation (3.2) thus yields

$$(a_1 + 1)P^{2n} - (a_1 - 1)Q^{2n} = 2$$

and so, via Theorem 1.1,  $P = Q = 1$ , contradicting  $p > 1$ .

We may thus suppose that  $b_1 = p^{n-1}s^n$  (so that, in particular,  $p$  fails to divide  $a_1 \cdot a_2$ , whence  $a_1$  and  $a_2$  are coprime). Then we have  $E_p = py_0^n$  for some positive integer  $y_0$  and so (3.1) implies that

$$E_{\frac{p+1}{2}} \pm E_{\frac{p-1}{2}} = pP^n \quad \text{and} \quad E_{\frac{p+1}{2}} \mp E_{\frac{p-1}{2}} = Q^n,$$

for  $P$  and  $Q$  positive integers. Applying (3.2) and (3.3), we thus have either

$$(a_1 + 1)p^2P^{2n} - (a_1 - 1)Q^{2n} = 2, \quad (a_1 + 1)p^2P^{2n} + (a_1 - 1)Q^{2n} = 2Ma^n$$

or

$$(a_1 + 1)Q^{2n} - (a_1 - 1)p^2P^{2n} = 2, \quad (a_1 + 1)Q^{2n} + (a_1 - 1)p^2P^{2n} = 2Ma^n.$$

It follows that

$$2(a_1 \pm 1)Q^{2n} \mp 2 = 2Ma^n.$$

If we suppose that  $a_1 = Mr^n$ , for some integer  $r$ , then

$$|(Mr^n \pm 1)Q^{2n} - Ma^n| = 1,$$

whereby, applying Theorem 1.1, we have  $Q = 1$ ,  $a = r$ , again a contradiction.

Finally, if  $a_1 \neq Mr^n$  for any integer  $r$ , then  $\gcd(M, a_2) > 1$ . Since we assume that  $P(M) \leq 13$ , it follows that  $a_2$  has a prime divisor in the set  $\{2, 3, 5, 7, 11, 13\}$ . As is well known, we may write

$$(3.6) \quad a_1 \cdot a_2 = T_p(a_1)$$

where  $T_p(x)$  is, again, the  $p$ th Tschebyscheff polynomial of the first kind. These satisfy the recursion

$$T_{2k+1}(x) = (4x^2 - 2)T_{2k-1}(x) - T_{2k-3}(x),$$

where  $T_1(x) = x$  and  $T_3(x) = 4x^3 - 3x$ . From this recursion, (3.6), and the fact that  $\gcd(a_1, a_2) = 1$ , it is easy to check that  $a_2$  is coprime to 210. For example, if we have  $a_1 \equiv \pm 1 \pmod{7}$ , then  $a_2 \equiv 1 \pmod{7}$  for all odd  $p$ , while  $a_1 \equiv \pm 2 \pmod{7}$  implies that  $a_2 \equiv 1 \pmod{7}$  if  $p \equiv \pm 1 \pmod{8}$ ,  $a_2 \equiv -1 \pmod{7}$  if  $p \equiv \pm 3 \pmod{8}$ . Finally, if  $a_1 \equiv \pm 3 \pmod{7}$ , then  $a_2 \equiv 1 \pmod{7}$  unless  $p = 3$  (whence  $a_2 \equiv -2 \pmod{7}$ ).

The situation modulo 11 or 13 is slightly more complicated. In each case, since  $p$  is an odd prime, we have, from the above recursion, that  $11 \mid a_2$  or  $13 \mid a_2$  only when  $p = 3$ . In this case,  $b_2 = 4a_1^2 - 1 = 3t^n$  for some integer  $t$  whereby, upon factoring, we deduce the existence of integers  $c$  and  $d$  for which  $c^n - 3d^n = 2$  with  $|cd| = t$ . It follows, from Theorem 1.1, that  $t = 1$ , contradicting  $a_1 > 1$ .

We are thus left to treat equation (3.4) with  $m = 2^\alpha$  for  $\alpha$  a nonnegative integer. Our claim will follow directly if we can show that  $\alpha = 0$ . If  $\alpha > 0$ , then there exist integers  $u$  and  $v$  for which

$$Ma^n + b^n\sqrt{B} = \left(u + v\sqrt{B}\right)^2,$$

whereby

$$(3.7) \quad 2u^2 - 1 = Ma^n$$

and

$$(3.8) \quad 2uv = b^n.$$

The first of these equations implies, since we assume  $3 \leq P(M) \leq 13$ , that  $M = 7^\beta$  for some positive integer  $\beta$ .

Now either  $u$  is even, in which case, from (3.8), there exist integers  $l$  and  $w$  for which  $u = 2^{n-1}l^n, v = w^n$ , or  $u$  is odd, whence  $u = l^n, v = 2^{n-1}w^n$ . In the first of these cases, from (3.7), we conclude that

$$2^{2n-1}l^{2n} - 7^\beta a^n = 1.$$

Arguing as in Kraus [7] (with minor complications at  $n = 5$  and  $n = 7$ ), this equation has no solutions with  $n \geq 5$  prime. Modulo 7, the same is true for  $n = 3$ . In the second case, we have

$$(3.9) \quad 2l^{2n} - 7^\beta a^n = 1,$$

where  $l$  is an odd integer. To treat this equation, we consider the Frey curve

$$E : Y^2 = X^3 + 2X^2 + 2l^{2n}X.$$

If  $p$  is a prime, coprime to  $14aln$ , define

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

For  $n \geq 11$  is prime, applying techniques of [4], there exists a weight 2, level 896 cuspidal newform  $f = \sum c_n q^n$  such that, if  $p$  is a prime, again coprime to  $14aln$ , we have

$$(3.10) \quad \text{Norm}_{K_f/\mathbb{Q}}(c_p - a_p) \equiv 0 \pmod{n}.$$

Similarly, if  $p \mid al$  but  $p$  fails to divide  $14n$ ,

$$(3.11) \quad \text{Norm}_{K_f/\mathbb{Q}}(c_p \pm (p+1)) \equiv 0 \pmod{n}.$$

From Stein's Modular Forms Database [12], we see that all the one dimensional forms at level 896 have  $c_3 = 0$ . A simple calculation shows that  $a_3 = 2$  for our Frey curve, provided 3 fails to divide  $l$  and hence one of (3.10) or (3.11) implies that  $f$  is not one dimensional. For the higher dimensional forms labelled (in Stein's notation) 5-12, we have  $c_3 = \theta$  with  $\theta^2 \pm 2\theta - 2 = 0$  or  $\theta^3 \pm 2\theta^2 - 6\theta \mp 8 = 0$ . Calculating with (3.10) and (3.11) shows that necessarily  $n = 11$  and  $3 \mid la$ . In this case, modulo 23, we have that  $11 \mid \beta$ , contradicting Theorem 1.1 (since the equation  $X^{11} - 2Y^{11} = 1$  has no solutions with  $|XY| > 1$ ).

To deal with the remaining values of  $n \in \{3, 5, 7\}$ , we employ (mostly) local considerations. For example, equation (3.9) has no solutions modulo 7, provided  $n = 3$ . For  $n = 5$ , considering (3.9) modulo 11, we find that necessarily  $5 \mid \beta$ . Since the equation  $X^5 - 2Y^5 = 1$  has, by Theorem 1.1, no solutions in integers  $X$  and  $Y$

with  $|XY| > 1$ , this leads to a contradiction. If  $n = 7$ , (3.9) is insoluble modulo 49 if  $\beta \geq 2$ . We are left then to deal with the Diophantine equation

$$2l^{14} - 7a^7 = 1.$$

Here, we may show that there are no local obstructions to solubility but employing, for instance, a “Thue-solver” such as that implemented in Simath, we find that there are, in fact no solutions in integers  $l$  and  $a$ . This completes the proof of Theorem 1.4.

#### 4. ACKNOWLEDGMENTS

The author would like to thank Wallapak Polasub for her insightful comments on an earlier version of this paper.

#### REFERENCES

- [1] M.A. Bennett, Rational approximation to algebraic numbers of small height : the Diophantine equation  $|ax^n - by^n| = 1$ , *J. Reine Angew Math.* 535 (2001), 1–49.
- [2] M.A. Bennett, The Diophantine inequality  $|ax^n - by^n| \leq 2$ , submitted for publication.
- [3] M.A. Bennett, Powers in recurrence sequences : Pell equations, *Trans. Amer. Math. Soc.*, to appear.
- [4] M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, **56** (2004), 23–54.
- [5] M.A. Bennett and P.G. Walsh, The Diophantine equation  $b^2x^4 - dy^2 = 1$ , *Proc. Amer. Math. Soc.* 127 (1999), 3481–3491.
- [6] A. Af Ekenstam, Contributions to the Theory of the Diophantine Equation  $Ax^n - By^n = C$ , Ph.D. Thesis, Uppsala, 1959.
- [7] A. Kraus, Majorations effectives pour l’équation de Fermat généralisée, *Canad. J. Math.* 49 (1997), no. 6, 1139–1161.
- [8] W. Ljunggren, A Diophantine equation with two unknowns, *C. R. Dixième Congrès Math. Scandinaves* 9146, 265–270.
- [9] W. Ljunggren, On an improvement of a theorem of T. Nagell concerning the diophantine equation  $Ax^3 + By^3 = C$ , *Math. Scan.* 1 (1953), 297–309.
- [10] J. Mueller and W. M. Schmidt, Trinomial Thue equations and inequalities, *J. Reine Angew. Math.* **379** (1987), 76–99.
- [11] T. Nagell, Solution complète de quelques équations cubiques à deux indéterminées, *J. de Math.* 4 (1925), 209–270.
- [12] W. Stein, Modular forms database, <http://modular.fas.harvard.edu/Tables/>
- [13] W. Tartakowsky, Auflösung der Gleichung  $x^4 - \rho y^4 = 1$ , *Bull. de l’Académie des Sciences URSS* 20 (1926), 310–324.
- [14] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory* **31** (1989), 99–132.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, B.C., V6T 1Z2 CANADA

*E-mail address:* `bennett@math.ubc.ca`