International Journal of Number Theory
Vol. 2, No. 2 (2006) 195–206

A GENERALIZATION OF A THEOREM OF BUMBY ON QUARTIC DIOPHANTINE EQUATIONS

MICHAEL A. BENNETT

Department of Mathematics, The University of British Columbia
1984 Mathematics Road Vancouver, B.C., Canada V6T 1Z2
bennett@math.ubc.ca

ALAIN TOGBÉ

Mathematics Department, Purdue University North Central
1401 S, U.S. 421, Westville IN 46391 USA
atogbe@pnc.edu

P. G. WALSH

Department of Mathematics, University of Ottawa
585 King Edward St., Ottawa, Ontario, Canada K1N-6N5
gwalsh@mathstat.uottawa.ca

Received 8 March 2005
Accepted 30 November 2005

Bumby proved that the only positive integer solutions to the quartic Diophantine equation $3X^4 - 2Y^2 = 1$ are $(X, Y) = (1, 1), (3, 11)$. In this paper, we use Thue's hypergeometric method to prove that, for each integer $m \geq 1$, the only positive integers solutions to the Diophantine equation $(m^2 + m + 1)X^4 - (m^2 + m)Y^2 = 1$ are $(X, Y) = (1, 1), (2m + 1, 4m^2 + 4m + 3)$.

Keywords: Thue equation; Pell equation; elliptic curve; hypergeometric function.

Mathematics Subject Classification 2000: 11D41, 11B39

1. Introduction

Given a parametrized family of cubic models of elliptic curves E_t over $\mathbb{Q}$, it is a notoriously difficult problem to find absolute bounds for the number of integral points on E_t (and, indeed, in many cases, it is unlikely such bounds even exist). Perhaps somewhat surprisingly, the situation is often radically different for quartic models. In a series of classical papers, Ljunggren (see e.g. [5] and the references therein) derived various explicit, absolute bounds for the number of integral solutions to quartic Diophantine equations. For example, he showed that, given positive integers a and b, the equation

$$aX^2 - bY^4 = 1$$

has at most a single solution in positive integers X and Y. The case of the apparently similar equation

$$aX^4 - bY^2 = 1 \tag{1.1}$$

is significantly more complicated (unless a is an integral square; see [1] and [4]). In fact, for general a and b, there is no absolute upper bound for the number of integral solutions to (1.1) available in the literature (unless one adds additional hypotheses; see [5]). Computations and assorted heuristics (see, e.g. [1], [4], [8], and [9]), however, suggest the following:

Conjecture 1.1. Let a and b be positive integers. Then Eq. (1.1) has at most two solutions in positive integers X and Y.

This conjectural upper bound is best possible since, choosing

$$(a, b) = (m^2 + m + 1, m^2 + m), \tag{1.2}$$

for m a positive integer, we find the solutions

$$(X, Y) = (1, 1) \text{ and } (X, Y) = (2m + 1, 4m^2 + 4m + 3) \tag{1.3}$$

to Eq. (1.1). One might even hypothesize that, in a certain sense we will make precise later, these pairs (a, b) (together with $(a, b) = (2, 1)$) are the only ones for which (1.1) has more than a single such solution.

In [2], Bumby applied a clever argument involving arithmetic in the quartic number field $\mathbb{Q}(\sqrt{-2}, \sqrt{-3})$ to verify Conjecture 1.1 for $(a, b) = (3, 2)$ (i.e. to show that the known solutions (1.3) are the only ones, in the simplest case $m = 1$ of (1.2)). Our goal in this paper is to deduce a like result for the entire family of pairs (a, b) in (1.2), that is, to prove

Theorem 1.2. *Let m be a positive integer. Then the only positive integral solutions to the equation*

$$(m^2 + m + 1)\, X^4 - (m^2 + m)\, Y^2 = 1 \tag{1.4}$$

are given by $(X, Y) = (1, 1)$ and $(X, Y) = (2m + 1, 4m^2 + 4m + 3)$.

Our argument is fundamentally different from that employed by Bumby [2]. In fact, the techniques of [2] do not apparently generalize to arbitrary values of $m > 1$. We will instead appeal to classical results of Thue [6] from the theory of Diophantine approximation. In the context of quartic equations, these were first utilized, independently, by Yuan [10] and by Chen and Voutier [3], to sharpen prior work of Ljunggren on Eq. (1.1), in case $b = 1$. In essence, this paper may be viewed as a companion piece to [7], where these techniques are applied in a somewhat more general setting.

2. Reduction to Thue Equations

As detailed in the introduction to [7], in order to bound the number of positive integer solutions to an equation of the form $aX^4 - bY^2 = 1$, it suffices to consider the case when $a = b + 1$. That is, it is sufficient to determine an upper bound for the number of integer solutions to Diophantine equations of the shape

$$(t+1)X^4 - tY^2 = 1. \tag{2.1}$$

In this context, a more precise version of Conjecture 1.1 is the following:

Conjecture 2.1. If $t > 1$ is integral, then the only positive integer solution to Eq. (2.1) is given by $(X, Y) = (1, 1)$, unless $t = m^2 + m$ for some positive integer m, in which case there is also the solution $(X, Y) = (2m + 1, 4m^2 + 4m + 3)$.

Our strategy in proving Theorem 1.2 will be as follows. We begin by recalling [7, Proposition 2.1], in which it was shown a positive integer solution of Eq. (2.1) gives rise to a solution to a Thue equation.

Proposition 2.2. *Let t be a positive integer. If there exists a solution to* (2.1) *in positive integers $(X, Y) \neq (1, 1)$, then there exists an integer solution (x, y) to the equation*

$$x^4 + 4tx^3y - 6tx^2y^2 - 4t^2xy^3 + t^2y^4 = t_0^2, \tag{2.2}$$

where t_0 divides t, $t_0 \leq \sqrt{t}$ and $\min\{|x|, |y|\} > 1$.

It follows, for such a solution, that x/y is “close” to one of the roots of the quartic polynomial

$$p_t(x) = x^4 + 4tx^3 - 6tx^2 - 4t^2x + t^2, \tag{2.3}$$

which we label $\beta^{(i)}$, $i = 1, 2, 3, 4$. For the special cases when $t = m^2 + m$ with m integral, we will be able to apply the hypergeometric method to obtain (nontrivial) effective measures of approximation for these roots, showing (eventually) that no such rational number x/y can exist.

In order to utilize the hypergeometric method, one requires good rational approximations to the roots $\beta^{(i)}, i = 1, 2, 3, 4$ of the polynomial (2.3). These roots are given explicitly by

$$\beta^{(1)} = \frac{\sqrt{t}}{\tau}(1+\rho), \quad \beta^{(2)} = \frac{\sqrt{t}}{\tau}(1-\rho), \quad \beta^{(3)} = (-\tau+\rho)\sqrt{t}, \quad \beta^{(4)} = -(\tau+\rho)\sqrt{t},$$

where

$$\tau = \sqrt{t+1} + \sqrt{t} \quad \text{and} \quad \rho = \sqrt{\tau^2+1}.$$

We will, here and henceforth, assume that $t = m^2 + m$, for m a positive integer. We may readily derive, via the Mean Value Theorem, the following inequalities for the roots $\beta^{(i)}$:

$$\begin{aligned} m+1+\frac{1}{8m^2}+\frac{1}{16m^3} &< \beta^{(1)} < m+1+\frac{1}{8m^2}+\frac{1}{8m^3}, \\ -m-\frac{1}{8m^2}+\frac{1}{16m^3} &< \beta^{(2)} < -m-\frac{1}{8m^2}+\frac{1}{8m^3}, \\ \frac{1}{4}-\frac{5}{64m^2}+\frac{1}{16m^3} &< \beta^{(3)} < \frac{1}{4}-\frac{5}{64m^2}+\frac{5}{64m^3}, \end{aligned} \tag{2.4}$$

and

$$-4m^2-4m-\frac{5}{4}+\frac{21}{64m^2}-\frac{21}{64m^3} < \beta^{(4)} < -4m^2-4m-\frac{5}{4}+\frac{21}{64m^2}-\frac{5}{16m^3}.$$

We will, in fact, apply the hypergeometric method of Thue and Siegel to obtain an effective measure of approximation to just the root $\beta^{(1)}$. Later, we will indicate why this is sufficient for our purposes.

3. Towards an Effective Measure of Approximation

Let us begin by recalling some notation. For a positive integer r, we put

$$X_r(X) = {}_2F_1(-r, -r-1/4; 3/4; X),$$

where ${}_2F_1$ denotes the classical hypergeometric function, and use X_r^* to denote the homogeneous polynomials derived from these polynomials, so that

$$X_r^*(X, Y) = Y^r X_r(X/Y). \tag{3.1}$$

A basic principle underlying the hypergeometric method and, indeed, a fundamental technique for proving irrationality in general, is the following folklore lemma (the formulation we provide here is Lemma 2.8 of [3]):

Lemma 3.1. *Let $\theta \in \mathbb{R}$. Suppose that there exist $k_0, l_0 > 0$ and $E, Q > 1$ such that for all $r \in \mathbb{N}$, there are rational integers p_r and q_r with $|q_r| < k_0 Q^r$ and $|q_r\theta - p_r| \le l_0 E^{-r}$ satisfying $p_r q_{r+1} \ne p_{r+1} q_r$. Then for any rational integers p and q with $|q| \ge 1/(2l_0)$, we have*

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{c|q|^{\kappa+1}}, \quad \textit{where} \quad c = 2k_0 Q (2l_0 E)^\kappa \ \textit{and}\ \kappa = \frac{\log Q}{\log E}.$$

This result says, in essense, that the existence of a dense set of suitably good rational approximations to a real number θ provides us with an explicit lower bound for rational approximation to θ. For our purposes, we will seek to apply this with $\theta = \beta^{(1)}$ (whereby, we need to improve upon the trivial lower bound given by Liouville's Theorem). The hypergeometric method is predicated on the idea of constructing the desired dense set of rational approximations through specializing rational functions (derived from the classical hypergeometric functions) at rational (or perhaps algebraic) values. We will generate these rational functions by appealing to the following special case of a result from [7] (cf. [3, Lemma 2.1]), which is essentially just a convenient formulation of the original work of Thue [6]. Note, in the notation of [3], we are taking $n = 4$,

$$U(x) = (x - \alpha_1)(x - \alpha_2), \quad P(x) = c_1(x - \alpha_1)^4 - c_2(x - \alpha_2)^4$$

and that the signs of $b(x)$ and $d(x)$ are reversed in comparison to [3].

Lemma 3.2. *Let α_1, α_2, c_1 and c_2 be complex numbers with $\alpha_1 \neq \alpha_2$ and define the following polynomials*

$$a(x) = \frac{5}{2}(\alpha_1 - \alpha_2)(x - \alpha_2), \quad c(x) = \frac{5}{2}\alpha_1(\alpha_1 - \alpha_2)(x - \alpha_2),$$

$$b(x) = \frac{5}{2}(\alpha_2 - \alpha_1)(x - \alpha_1), \quad d(x) = \frac{5}{2}\alpha_2(\alpha_2 - \alpha_1)(x - \alpha_1),$$

$$u = u(x) = -c_2(x - \alpha_2)^4 \quad \text{and} \quad z = z(x) = c_1(x - \alpha_1)^4.$$

Putting $\sqrt{\lambda} = (\alpha_1 - \alpha_2)/2$, we write, for a positive integer r,

$$(\sqrt{\lambda})^r A_r(x) = a(x)X_r^*(z, u) + b(x)X_r^*(u, z)$$

and

$$(\sqrt{\lambda})^r B_r(x) = c(x)X_r^*(z, u) + d(x)X_r^*(u, z).$$

Then, for any root β of $P(x) = z(x) - u(x)$, the polynomial

$$C_r(x) = \beta A_r(x) - B_r(x)$$

is divisible by $(x - \beta)^{2r+1}$.

We will apply this by choosing α_1, α_2, c_1 and c_2 so that $P(x) = p_t(x)$ and $\beta = \beta^{(1)}$. Since $\beta^{(1)}$ is extremely close to $m + 1$, it follows that

$$B_r(m + 1)/A_r(m + 1)$$

corresponds to a good rational approximation to $\beta^{(1)}$. In order to use Lemma 3.1, we need to bound $|A_r(m + 1)|$, $|B_r(m + 1)|$ and $|C_r(m + 1)|$. We will do this via special cases of [3, Lemmas 2.5 and 2.6], and [7, Lemma 3.4] (the last to treat non-archimedean valuations):

Lemma 3.3. *With the above notation, put $w(x) = z(x)/u(x)$ and write $w(x) = \mu e^{i\varphi}$ with $\mu \geq 0$ and $-\pi < \varphi \leq \pi$. Put $w(x)^{1/4} = \mu^{1/4} e^{i\varphi/4}$.*

(i) *For any non-zero $x \in \mathbb{C}$ such that $w = w(x)$ is not a negative real number or zero,*

$$(\sqrt{\lambda})^r C_r(x) = \{\beta(a(x)w(x)^{1/4} + b(x)) - (c(x)w(x)^{1/4} + d(x))\}X_r^*(u, z) - (\beta a(x) - c(x))u(x)^r R_r(w),$$

with

$$R_r(w) = \frac{\Gamma(r + 5/4)}{r!\,\Gamma(1/4)} \int_1^w ((1 - t)(t - w))^r t^{-r-3/4}\, dt,$$

where the integration path is the straight line from 1 to w.

(ii) *Let* $w = e^{i\varphi}, 0 < \varphi < \pi$ *and put* $\sqrt{w} = e^{i\varphi/2}$. *Then*

$$|R_r(w)| \leq \frac{4\,\Gamma(r+5/4)}{r!\,\Gamma(1/4)}\varphi|1-\sqrt{w}|^{2r}.$$

Lemma 3.4. *Let* u, w *and* z *be as above. Then*

$$|X_r^*(u,z)| \leq 4\,|u|^r\,\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)}\,|1+\sqrt{w}|^{2r-2}.$$

Lemma 3.5. *Let* N_r *be the greatest common divisor of the numerators of the coefficients of* $X_r(1-2x)$ *and let* D_r *be the least common multiple of the denominators of the coefficients of* $X_r(x)$. *Then the polynomial* $(D_r/N_r)X_r(1-2x)$ *has integral coefficients. Moreover,* $N_r = 2^r$,

$$D_r\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)} < 0.8397 \cdot 5.342^r \quad \text{and} \quad D_r\frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} < 0.1924 \cdot 5.342^r.$$

Finally, in order to guarantee that the rational approximations we produce are essentially distinct, we will have need of [3, Lemma 2.7]:

Lemma 3.6. *Let* $\alpha_1, \alpha_2, A_r(X), B_r(X)$ *and* $P(X)$ *be defined as in Lemma* 3.1 *and let* a, b, c *and* d *be complex numbers satisfying* $ad - bc \neq 0$. *Define*

$$K_r(X) = aA_r(X) + bB_r(X) \quad \text{and} \quad L_r(X) = cA_r(X) + dB_r(X).$$

If $(x-\alpha_1)(x-\alpha_2)P(x) \neq 0$, *then*

$$K_{r+1}(x)L_r(x) \neq K_r(x)L_{r+1}(x),$$

for all $r \geq 0$.

We now determine the quantities defined in Lemma 3.2. Choose

$$\alpha_1 = \sqrt{-t}, \quad \alpha_2 = -\sqrt{-t}, \quad c_1 = (1+\sqrt{-t})/2,\ c_2 = (1-\sqrt{-t})/2,$$

whereby $\lambda = -t$ and $P(x) = p_t(x)$, as in (2.3). We will now show how our various lemmas may be employed to obtain an effective measure of approximation to $\beta^{(1)}$. Let us select $x = m+1$ and define

$$\eta = 1 + i\sqrt{m^2+m}(4m^2+4m+3).$$

It follows that

$$w = w(m+1) = \frac{-1+i(4m^2+4m+3)\sqrt{m^2+m}}{1+i(4m^2+4m+3)\sqrt{m^2+m}} = -\frac{\overline{\eta}}{\eta},$$

and so

$$w^{1/4} = \frac{1+i\tau}{\rho} \cdot \frac{m+1-i\sqrt{m^2+m}}{m+1+i\sqrt{m^2+m}}. \tag{3.2}$$

Using the fact that $\rho^2 = \tau^2 + 1$, one may check that

$$a(m+1) = -5(m+1)[m - i\sqrt{m^2+m}] = \overline{b(m+1)}$$

and

$$c(m+1) = -5m(m+1)[m+1+i\sqrt{m^2+m}] = \overline{d(m+1)},$$

whereby

$$\beta^{(1)} = \frac{c(m+1)w^{1/4} + d(m+1)}{a(m+1)w^{1/4} + b(m+1)},$$

and hence the first term in the expression for $(-t)^{r/2}C_r(m+1)$ in Lemma 3.3 vanishes. By Lemmas 3.2 and 3.3, we thus have that

$$\begin{aligned} (-t)^{r/2}A_r(m+1) &= a(m+1)X_r^*(z(m+1), u(m+1)) \\ &\quad + b(m+1)X_r^*(u(m+1), z(m+1)), \\ (-t)^{r/2}B_r(m+1) &= c(m+1)X_r^*(z(m+1), u(m+1)) \\ &\quad + d(m+1)X_r^*(u(m+1), z(m+1)), \\ (-t)^{r/2}C_r(m+1) &= -(\beta^{(1)}a(m+1) - c(m+1))[u(m+1)]^r R_r(w). \end{aligned} \tag{3.3}$$

These quantities form the basis for our sequence of rational approximations to $\beta^{(1)}$. We first eliminate some common factors. One can check that

$$u(m+1) = -\frac{1}{2}(m+1)^2\eta = -\overline{z(m+1)}, \tag{3.4}$$

$$\frac{z(m+1)}{u(m+1)} = 1 - \frac{2}{\eta} \quad \text{and} \quad \frac{u(m+1)}{z(m+1)} = 1 - \frac{2}{\overline{\eta}}. \tag{3.5}$$

Using (3.1), (3.4), and (3.5), we obtain

$$X_r^*(z(m+1), u(m+1)) = (-1)^r \, \frac{1}{2^r} \, (m+1)^{2r} \, \eta^r \, X_r\left(1 - \frac{2}{\eta}\right)$$

and

$$X_r^*(u(m+1), z(m+1)) = \frac{1}{2^r} \, (m+1)^{2r} \, \overline{\eta}^r \, X_r\left(1 - \frac{2}{\overline{\eta}}\right).$$

After some routine manipulations, we find, from (3.3) and Lemma 3.5, considering the cases of r even or odd separately, that the quantities

$$P_r = \frac{m^{[(r-2)/2]}D_rB_r(m+1)}{10(m+1)^{[3r/2+1]}} \quad \text{and} \quad Q_r = \frac{m^{[(r-2)/2]}D_rA_r(m+1)}{10(m+1)^{[3r/2+1]}} \tag{3.6}$$

are rational integers. Note that we have

$$Q_r\beta^{(1)} - P_r = S_r, \tag{3.7}$$

where

$$S_r = \frac{m^{[(r-2)/2]}D_rC_r(m+1)}{10(m+1)^{[3r/2+1]}}. \tag{3.8}$$

The integers defined by (3.6) are those whose quotients will provide us with our rational approximations to $\beta^{(1)}$. We want to show that these are "good" approximations; to do this, we will estimate $|Q_r|$ and $|S_r|$ from above. From (3.2), we may write

$$w^{1/4} = \frac{1}{(2m+1)\rho}[(1+2\tau\sqrt{t}) + i(\tau - 2\sqrt{t})],$$

whereby

$$w^{1/2} = \frac{1}{(2m+1)^2\rho^2}[(1+2\tau\sqrt{t})^2 - (\tau-2\sqrt{t})^2 + 2i(1+2\tau\sqrt{t})(\tau-2\sqrt{t})].$$

It is easy to verify via calculus that

$$1.999 < |1+\sqrt{w}| < 2, \quad \text{for } m \geq 2, \tag{3.9}$$

and similarly that

$$|u(m+1)(1+\sqrt{w})^2| < 23.266\, m^5, \tag{3.10}$$

at least provided $m \geq 3$. From the expressions for $a(m+1), b(m+1), c(m+1)$ and $d(m+1)$, one can see that

$$|a(m+1)| = |b(m+1)| = 5(m+1)\sqrt{m(2m+1)} \tag{3.11}$$

and

$$|c(m+1)| = |d(m+1)| = 5m(m+1)\sqrt{(m+1)(2m+1)}. \tag{3.12}$$

By (3.3), (3.11), the fact that $|z| = |u|$ (from 3.4), and Lemma 3.4, we have that

$$t^{r/2}|A_r(m+1)| \leq 8\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)}\,|a(m+1)|\,|u(m+1)|^r\,|1+\sqrt{w}|^{2r-2}$$

whereby, from (3.9), (3.10), and (3.11),

$$t^{r/2}|A_r(m+1)| \leq 10.011\frac{\Gamma(3/4)r!}{\Gamma(r+3/4)}\,(m+1)\sqrt{m(2m+1)}(23.266\, m^5)^r.$$

Now we use (3.6) and Lemma 3.5 to obtain

$$|Q_r| < \frac{0.841}{m}\sqrt{m(2m+1)}(124.287\, m^3)^r < 1.285(124.287\, m^3)^r, \tag{3.13}$$

for $m \geq 3$.

Next, we look to bound $|S_r|$. By (3.3),

$$t^{r/2}|C_r(m+1)| = |\beta^{(1)}a(m+1) - c(m+1)|\,|u(m+1)|^r\,|R_r(w(m+1))|$$

and so, from Lemma 3.3 and the fact that $c(m+1)/a(m+1) = i\sqrt{t}$, it follows that

$$t^{r/2}|C_r(m+1)| < |a(m+1)||\beta^{(1)} - i\sqrt{t}|\,\frac{4\,\Gamma(r+5/4)}{r!\,\Gamma(1/4)}\,\varphi\,|u(m+1)(1-\sqrt{w})^2|^r,$$

with φ as defined in Lemma 3.3. Since

$$\sin\varphi = \operatorname{Im}\, w = \frac{2\sqrt{m^2+m}(4m^2+4m+3)}{1+(m^2+m)(4m^2+4m+3)^2},$$

we have that $\varphi < 1/(2m^3)$. Therefore, from the bounds for $\beta^{(1)}$ in (2.4),

$$\varphi|\beta^{(1)} - i\sqrt{m^2+m}| < \frac{0.885}{m^2},$$

for $m \geq 3$. As above, a routine application of calculus yields

$$|u(m+1)(1-\sqrt{w(m+1)})^2| \leq \frac{0.136}{m},$$

again, for $m \geq 3$. From these results, (3.8) and Lemma 3.5, one can see that

$$|S_r| \leq \frac{0.394}{m^2}(1.376\, m^3)^{-r}. \tag{3.14}$$

We are now in position to derive our desired lower bound for rational approximation to $\beta^{(1)}$:

Theorem 3.7. *Suppose that* $m \geq 3$. *Define*

$$\kappa = \frac{\log(124.287\, m^3)}{\log(1.376\, m^3)}.$$

If p *and* q *are positive integers, then*

$$\left|\beta^{(1)} - \frac{p}{q}\right| > \frac{1}{319.42\, m^3(1.09\, m)^{\kappa} q^{1+\kappa}}.$$

Proof. We apply Lemma 3.1. First, notice that $P_rQ_{r+1} - P_{r+1}Q_r$ is a non-zero multiple of

$$A_{r+1}(m+1)B_r(m+1) - A_r(m+1)B_{r+1}(m+1).$$

From Lemma 3.6, with $a = d = 1$, $b = c = 0$ and $x = m+1$, it follows that $P_rQ_{r+1} \neq P_{r+1}Q_r$, and thus, using (3.7), we may invoke Lemma 3.1, with $p_r = P_r$ and $q_r = Q_r$. For $m \geq 3$, from (3.13) and (3.14), we can take $k_0 = 1.285$, $l_0 = 0.394\, m^{-2}$, $E = 1.376\, m^3$ and $Q = 124.287\, m^3$. Lemma 3.1 thus yields the desired result. □

4. Proof of Theorem 1.2

To prove Theorem 1.2, let us begin by defining, for non-negative integers k, a sequence of polynomials $\{V_{2k+1}(t)\}$ via the relation

$$(\sqrt{t+1}+\sqrt{t})^{2k+1} = V_{2k+1}(t)\sqrt{t+1} + W_{2k+1}(t)\sqrt{t}.$$

For future use, we will also define

$$(\sqrt{t+1}+\sqrt{t})^{2k} = T_k(t) + U_k(t)\sqrt{t(t+1)}.$$

Given an integer $t \geq 1$, a positive integer solution (X, Y) to the quartic Diophantine equation (2.1) is equivalent, by the classical theory of Pell equations, to an index $k \geq 0$ for which $X^2 = V_{2k+1}(t)$. In [7], the authors showed that for all $k \geq 1$, the equation $X^2 = V_{4k+1}(t)$ has no solutions in positive integers X and t. It remains, therefore, to derive an analogous result for the equation $X^2 = V_{4k+3}(t)$. As noted in [7], a solution to this latter equation corresponds to a rational x/y for which the closest root of the polynomial p_t is either $\beta^{(1)}$ or $\beta^{(2)}$. Let us now estimate how close such a rational number *must* be in order that (x, y) is a solution of (2.2).

We begin by proving a lower bound for $|y|$ in terms of m, through what is essentially an application of Runge's method. For $1 \leq k \leq 24$, we compute the Puiseux expansions at infinity of the algebraic function $z(m)$ defined by $z^2 = V_{4k+3}(m^2 + m)$ and find, for each k, a positive integer r_k and integer polynomials $f_{4k+3}(m), g_{4k+3}(m)$ with the property that

$$2^{2r_k} V_{4k+3}(m^2 + m) = (f_{4k+3}(m))^2 + g_{4k+3}(m),$$

with $2 \deg f_{4k+3}(m) = \deg V_{4k+3}(m^2 + m) = 4k + 2$, and $\deg g_{4k+3}(m) = 2k$. We verify that each of the polynomials $g_{4k+3}(m)$ has no positive integer roots. We then notice that $|f_{4k+3}(m)| > |g_{4k+3}(m)|$ for $m > 0$, a much stronger condition than required. We remark that, if one could prove that this property holds for all $k \geq 1$, this would yield a completely different proof of Theorem 1.2. In any case, it follows from the above properties that each of the equations $z^2 = V_{4k+3}(m^2 + m)$, $(1 \leq k \leq 24)$, has no solutions in positive integers (z, m).

To finish deriving our lower bound for $|y|$, we begin by noting that a short calculation yields the inequalities

$$0.9\, \tau^{k-1} < V_k \leq \tau^{k-1}, \tag{4.1}$$

valid for $m \geq 3$ and $k \geq 3$. We will mimic the proof of [7, Proposition 2.1]. Let us begin by noting the relation

$$V_{4k+3} = V_{2k+1}^2 + V_{2k+2}^2 = (T_k + tU_k)^2 + tU_{k+1}^2,$$

valid for all $k \geq 0$. From the supposition that

$$X^2 = V_{4k+3},$$

we thus have

$$tU_{k+1}^2 = X^2 - (T_k + tU_k)^2$$

and hence, from the coprimality of U_k and $T_k + tU_k$ and the parity of U_k, we deduce the existence of positive integers G, H, t_1 and t_2 with $U_{k+1} = 2GH$, $t = t_1 t_2$, and

$$X - (T_k + tU_k) = 2t_1 G^2, \quad X + (T_k + tU_k) = 2t_2 H^2.$$

Substituting for T_k and U_k in the equation $T_k^2 - t(t+1)U_k^2 = 1$ and setting $t_0 = \min\{t_1, t_2\}$ and either $(x, y) = (t_1 G, H)$ or $(-t_2 H, G)$ leads us to Eq. (2.2).

We will suppose that $|y| = G$, as the case $|y| = H$ may be treated in a similar fashion, and actually leads to a larger lower bound for $|y|$. It is easy to see that

$$\sqrt{V_{4k+3}} - V_{2k+1} = \frac{V_{2k+2}}{\sqrt{(V_{2k+1}/V_{2k+2})^2 + 1} + (V_{2k+1}/V_{2k+2})},$$

and so, from (4.1), we deduce the inequalities

$$2t_1 y^2 > \frac{1}{4}\,\tau^{2k+1} > 2^{2k-1}(\sqrt{t})^{2k+1}.$$

Since $t_1 \leq t$, $m < \sqrt{t}$ and $k \geq 25$, we thus have that

$$|y| > 2^{24}\, m^{24}. \tag{4.2}$$

We now estimate how close x/y must be to one of $\beta^{(1)}$ or $\beta^{(2)}$. From (4.2), we can evidently assume that $|y| \geq 4$. Let us suppose first that (x, y) is a solution of Eq. (2.2) with $\beta^{(1)}$ closest to x/y. In this case, we may assume that $|x - \beta^{(1)} y| \leq t^{1/4}$, otherwise $y^4 |p_t(x/y)| > t$. Thus x/y is greater than $\beta^{(1)} - t^{1/4}/4$, whence

$$\left|\beta^{(2)} - \frac{x}{y}\right| > \beta^{(1)} - \beta^{(2)} - \frac{1}{4} m^{1/2} > 2m - \frac{1}{4} m^{1/2} + 1 - \frac{1}{4} m^{-1/2},$$

by the third and fourth inequalities in (2.4). Similarly, we have that

$$\left|\beta^{(3)} - \frac{x}{y}\right| > m - \frac{1}{4} m^{1/2} + \frac{3}{4} + \frac{9}{64m^2}, \quad \left|\beta^{(4)} - \frac{x}{y}\right| > 4m^2 + 5m - \frac{1}{4} m^{1/2} + \frac{9}{4} + \frac{13}{64m^2},$$

and, upon combining the above and assuming that $m \geq 3$,

$$\prod_{i \neq 1} \left|\beta^{(i)} - \frac{x}{y}\right| > 7.8\, m^4.$$

Therefore, if $|p_t(x, y)| = t_0^2 \leq t$, with $t = m^2 + m$ and $m \geq 3$, then

$$\left|\beta^{(1)} - \frac{x}{y}\right| < \frac{1}{5.85\, m^2\, y^4}. \tag{4.3}$$

Conversely, if the closest root to x/y is $\beta^{(2)}$, then, arguing in a similar fashion, we have

$$\left|\beta^{(2)} - \frac{x}{y}\right| < \frac{1}{5.85\, m^2\, y^4}.$$

Since $\beta^{(1)} \beta^{(2)} = -t$, a short calculation shows that

$$\left|\beta^{(1)} - \left(\frac{-ty}{x}\right)\right| < \frac{m^2}{5.8\, x^4}. \tag{4.4}$$

It follows, in either case (4.3) or (4.4), that there exist positive integers p and q, such that

$$\left|\beta^{(1)} - \frac{p}{q}\right| < \frac{m^2}{5.8\, q^4}.$$

Combining this with Theorem 3.7, we thus have that

$$q^{3-\kappa} < \frac{319.42\, m^5}{5.8}(1.09\, m)^{\kappa}, \tag{4.5}$$

provided that $m \geq 3$. Combining (4.5) with the lower bound for $|y|$ in (4.2) contradicts our choice of $m \geq 3$. For $m = 1$, we may appeal to [2], while, for $m = 2$, we may apply the computer package KANT (*ThueSolve*, to be precise) to the Thue equations

$$x^4 + 24x^3y - 36x^2y^2 - 144xy^3 + 36y^4 \in \{1, 4\}.$$

The only solutions we encounter are with $(x, y) = \pm(2, -1), \pm(1, 0)$. This, with Proposition 2.2, completes the proof of Theorem 1.2.

Acknowledgment

The first and third authors gratefully acknowledge support from the Natural Sciences and Engineering Research Council of Canada. The second author acknowledges support from Purdue University North Central.

References

[1] M. A. Bennett and P. G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$, *Proc. A.M.S.* **127** (1999) 3481–3491.

[2] R. T. Bumby, The Diophantine equation $3x^4 - 2y^2 = 1$, *Math. Scand.* **21** (1967) 144–148.

[3] J. H. Chen and P. M. Voutier, A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quartic Thue equations, *J. Number Theory* **62** (1997) 71–99.

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

[5] W. Ljunggren, On the Diophantine equation $Ax^4 - By^2 = C (C = 1, 4)$, *Math. Scand.* **21** (1967) 149–158.

[6] A. Thue, Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen, *J. Reine Angew. Math.* **138** (1910) 96–108.

[7] A. Togbé, P. M. Voutier and P. G. Walsh, Solving a family of Thue equations with an application to the equation $x^2 - dy^4 = 1$, *Acta Arith.* **120**(1) (2005) 39–58.

[8] P. G. Walsh, Diophantine equations of the form $aX^4 - bY^2 = \pm 1$, in *Algebraic Number Theory and Diophantine Analysis*, Proceedings of the International Conference in Graz 1998 (Walter de Gruyter, Berlin 2000), pp. 531–554.

[9] P. G. Walsh, A note on Ljunggren's theorem about the Diophantine equation $aX^2 - bY^4 = 1$, *Comptes Rendues Math. Rep. Acad. Sci. Canada* **20** (1998) 113–119.

[10] P. Yuan, Rational and algebraic approximations of algebraic numbers and their application, *Sci. China Ser. A* **40** (1997) 1045–1051.