Bull. Aust. Math. Soc. **82** (2010), 187–204
doi:10.1017/S0004972710000377

ON THE DIOPHANTINE EQUATION $z^2 = f(x)^2 \pm f(y)^2$, II

BO HE, ALAIN TOGBÉ✉ and MACIEJ ULAS

(Received 20 October 2009)

Abstract

Let $f \in \mathbb{Q}[X]$ and let us consider a Diophantine equation $z^2 = f(x)^2 \pm f(y)^2$. In this paper, we continue the study of the existence of integer solutions of the equation, when the degree of f is 2 and if $f(x)$ is a triangular number or a tetrahedral number.

2000 *Mathematics subject classification*: primary 11D25; secondary 11D41.

Keywords and phrases: Pythagorean triples, Diophantine equations.

1. Introduction

Let $f \in \mathbb{Q}[X]$ and let us consider the Diophantine equation

$$z^2 = f(x)^2 \pm f(y)^2. \tag{1.1}$$

We are interested in the existence of infinitely many rational solutions (x, y, z) of Equation (1.1). A similar problem was studied by the third author in [5]. In fact, he considered the Diophantine equation

$$f(x)f(y) = f(z)^2, \tag{1.2}$$

where $f \in \mathbb{Q}[X]$ is a polynomial function and $\deg f \leq 3$. In [5], he proved that if f is a quadratic function, then the Diophantine equation $f(x)f(y) = f(z)^2$ has infinitely many nontrivial solutions in $\mathbb{Q}(t)$. Let us recall that a triple (x, y, z) of rational numbers is a nontrivial solution of Equation (1.2) if $f(x) \neq f(y)$ and $f(z) \neq 0$. In the case where f is a cubic polynomial function of the form $f(X) = X(X^2 + aX + b)$, a, b being nonzero integers such that if $p \mid a$, then $p^2 \nmid b$, he showed that for all but finitely many integers a, b satisfying these conditions, Equation (1.2) has infinitely many nontrivial solutions in the rational numbers.

The first author was supported by the Applied Basic Research Foundation of Sichuan Provincial Science and Technology Department (No. 2009JY0091). The second author thanks Purdue University North Central for the support. The third author was supported by START for young scientists, founded by the Polish Science Foundation.

In [6], the second and third authors studied Equation (1.1). Equations of this type have a strong geometric flavour. Indeed, each nontrivial solution (that is, with $f(x)f(y) \neq 0$) of the equation $z^2 = f(x)^2 + f(y)^2$ gives a right triangle with legs of length $f(x)$, $f(y)$ and hypotenuse z. Similarly, each nontrivial solution (that is, $f(x)^2 \neq f(y)^2$) of the equation $z^2 = f(x)^2 - f(y)^2$ gives a right triangle with legs z, $f(y)$ and hypotenuse $f(x)$. They considered Equation (1.1) under the assumption that f is a polynomial of degree two with rational coefficients. It is obvious to observe that one can consider a polynomial of the form $f(X) = X^2 + a$, $a \neq 0$. They proved that if there exists a rational number t_0 such that the set of rational points on the quartic curve $V^2 = (U^2 + a)^2 + (t_0^2 + a)^2$ is infinite then the set of rational parametric solutions of the equation $z^2 = (x^2 + a)^2 + (y^2 + a)^2$ is nonempty. In fact, without much effort it is possible to show that the set of rational parametric solutions is infinite. Next, they proved that if f is of degree two and has two distinct roots over the field $\mathbb{C}$ then the surface related to the Diophantine equation $z^2 = f(x)^2 - f(y)^2$ is unirational over the field $\mathbb{Q}$. Moreover, they considered a quadratic polynomial of the form $f(X) = (aX + b)(cX + d)$ where $a, b, c, d \in \mathbb{Z}$ and they proved that if $b/a \neq d/c$ then the quartic equation $f(z)^2 = f(x)^2 + f(y)^2$ has infinitely many rational parametric solutions.

They also studied a cubic polynomial of the form $f(X) = X(X^2 + aX + b)$ with $a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$ and proved that Equation (1.1) has infinitely many solutions in $\mathbb{Q}(t)$. With polynomials of the form $f(x) = X^3 + aX^2 + b$, $a \neq 0$, they obtained a similar result for the equation $z^2 = f(x)^2 - f(y)^2$. Finally, they considered the equation $z^2 = f(x)^2 - f(y)^2$ with $f(x) = x^4 + a$, $a \neq 0$. Under some additional assumptions they proved that the set of rational solutions of this equation is infinite.

In this paper, we study the system of equations

$$z^2 = (x^2 + a)^2 \pm y^2 = x^2 \pm (y^2 + a)^2.$$

We find the solutions in all cases (see Section 2). Then we continue the study of Equation (1.1) when $f(x) = x^2 + a$ but using properties of Pell equations (see Section 3). In this case, when $a = -\tau^2$ for example, Equation (1.1) has infinitely solutions, which are determined explicitly. In general, we do not always have infinitely many solutions but we give the conditions for the existence of solutions by the means of Diophantine approximations. We find the solutions to Equation (1.1) for some particular cases. Finally, in Section 4, we investigate Equation (1.1) when $f(x)$ is a triangular number t_x or a tetrahedral number T_x. Firstly, we prove that the equation $z^2 = t_x^2 + t_y^2$ has infinitely many solutions in polynomials $x(u), y(u), z(u) \in \mathbb{Z}[u]$ that satisfy the condition $\mathrm{GCD}(t_{x(u)}, t_{y(u)}) = 1$. In fact, all solutions given by Sierpiński satisfy the condition $\mathrm{GCD}(t_x, t_y) > 1$. Secondly, we show that the equation $T_x^2 + T_y^2 = z^2$ has infinitely many integer solutions satisfying the condition $y - x = 1$. Moreover, we prove that there exists an infinite sequence of solutions (x_n, y_n, z_n) of the equation $T_x^2 + T_y^2 = z^2$ such that $y_n - x_n \to \infty$. Finally, we show that the set of

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

integer solutions of the system of equations

$$z_1^2 = T_x^2 + T_y^2, \quad z_2^2 = T_x^2 + T_{y+1}^2$$

is infinite.

2. The equation $z^2 = (x^2 + a)^2 \pm y^2 = x^2 \pm (y^2 + a)^2$

The equations $Z^2 = f(X)^2 \pm Y^2$ with $f(X) = AX^2 + BX + C$, $A \neq 0$, $\Delta_f = B^2 - 4AC \neq 0$, can be rewritten in the form

$$z^2 = (x^2 + a)^2 \pm y^2, \tag{2.1}$$

where

$$x = 2AX + B, \quad y = 4AY, \quad z = 4AZ, \quad a = -\Delta_f.$$

Analogously, equations $Z^2 = X^2 \pm f(Y)^2$ with $x = 4AX$ and $y = 2AY + B$ instead, but with other definitions as above, can be rewritten in the form

$$z^2 = x^2 \pm (y^2 + a)^2. \tag{2.2}$$

One can verify that (2.1) or (2.2) has infinitely many positive integer solutions (x, y, z). To see this, start with the primitive solutions of $Z^2 = X^2 + Y^2$ that are given by

$$X = 2mn, \quad Y = m^2 - n^2, \quad Z = m^2 + n^2, \quad \mathrm{GCD}(m, n) = 1,$$

where one of m and n is odd and the other is even. Equations (2.1) and (2.2) have solutions

$$x^2 + a = m^2 \pm n^2, \quad y^2 + a = m^2 - n^2.$$

We only need to consider the first equation. In fact, the result for the weaker Waring problem for degree two implies that the equation $a = m^2 \pm n^2 - x^2$ always has nonzero solutions m, n, x for any nonzero integer a.

We consider four possibilities for the simultaneous equations

$$z^2 = (x^2 + a)^2 \pm y^2 = x^2 \pm (y^2 + a)^2. \tag{2.3}$$

The first possibility gives us the following result.

THEOREM 2.1. *The equations*

$$z^2 = (x^2 + a)^2 + y^2 = x^2 + (y^2 + a)^2 \tag{2.4}$$

have no positive integer solutions with $x \neq y$, if $a \geq -1$ or the square-free part of $2a - 1$ has a prime divisor of the form $4k + 3$.

PROOF. From the second equation of (2.4),

$$(x^2 - y^2)(x^2 + y^2 + 2a - 1) = 0.$$

Suppose that x and y are positive integers such that $x \neq y$. Then

$$-(2a - 1) = x^2 + y^2. \tag{2.5}$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

When $a \geq 0$, we get the contradiction $2 \leq x^2 + y^2 \leq 1$. By [3, Theorem 366, p. 299], we know that if $-(2a-1) = n_1^2 n_2$ with n_2 square-free, then every prime divisor of n_2 is of the form $4k+1$. □

For which values of a do Equations (2.4) have positive integer solutions? The answer is given by the following result.

THEOREM 2.2. *If*

$$a = -(Q_{2s}^2 Q_{2t-1}^2 + 4P_{2s}^2 P_{2t-1}^2 - 1)/2$$

with $s, t \geq 1$, *then Equations* (2.4) *have positive integer solutions*

$$(x, y, z) = (Q_{2s}Q_{2t-1}, 2P_{2s}P_{2t-1}, P_{2s}^2 + P_{2t-1}^2),$$

where the kth Pell numbers satisfy $Q_k^2 - 2P_k^2 = (-1)^k$.

PROOF. From Equation (2.5),

$$x^2 + a = x^2 - \frac{x^2+y^2-1}{2} = \frac{x^2-y^2+1}{2}.$$

The first equation of (2.4) has solution

$$x^2 + a = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

So

$$x^2 - y^2 + 1 = 2m^2 - 2n^2$$

gives us

$$x^2 = 4m^2n^2 + 2m^2 - 2n^2 - 1 = (2m^2-1)(2n^2+1).$$

The above equation has positive integer solutions such that

$$x_1^2 - 2m^2 = -1, \quad x_2^2 - 2n^2 = 1, \quad x = x_1x_2.$$

The kth Pell numbers satisfy

$$Q_k^2 - 2P_k^2 = (-1)^k.$$

Thus

$$x_1 = Q_{2t-1}, \quad m = P_{2t-1}, \quad x_2 = Q_{2s}, \quad n = P_{2s}.$$

This implies that

$$x = Q_{2s}Q_{2t-1}, \quad y = 2P_{2s}P_{2t-1}, \quad z = P_{2s}^2 + P_{2t-1}^2$$

with $a = -(x^2+y^2-1)/2$. This completes the proof of the theorem. □

A special example is obtained by setting $s = t = 1$ in Theorem 2.2. As $P_1 = 1$, $P_2 = 2$, $Q_1 = 1$ and $Q_2 = 3$, we have $a = -12$ and $(x, y, z) = (3, 4, 5)$. The solution satisfies the system of equations

$$z^2 = (x^2+a)^2 + y^2 = x^2 + (y^2+a)^2 = x^2 + y^2. \tag{2.6}$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

This example leads us to find a for which Equations (2.6) have positive integer solutions. In fact, letting $t = s$ or $t = s + 1$, and $k = \min\{2s, 2t - 1\}$, we obtain the following result.

THEOREM 2.3. *If $a = -(Q_{2k+1}^2 - 1)/4$ for $1 \le k \in \mathbb{N}$, then Equations (2.6) have positive integer solutions*

$$(x, y, z) = ((Q_{2k+1} + 1)/2, (Q_{2k+1} - 1)/2, P_{2k+1}).$$

PROOF. Let $t = s$ or $s + 1$ in Theorem 2.2 and $k = \min\{2s, 2t - 1\}$. Then

$$a = -\frac{Q_k^2 Q_{k+1}^2 + 4P_k^2 P_{k+1}^2 - 1}{2}.$$

In order to obtain the value of a in the theorem, we need to show that

$$Q_{2k+1}^2 = 2Q_k^2 Q_{k+1}^2 + 8P_k^2 P_{k+1}^2 - 1. \tag{2.7}$$

By the well-known identities

$$Q_m Q_n + 2P_m P_n = Q_{m+n}, \quad Q_m Q_n - 2P_m P_n = (-1)^n Q_{m-n}, \tag{2.8}$$

if we take $m = k + 1$, $n = k$, the left-hand side of (2.7) equals $(Q_k Q_{k+1} + 2P_k P_{k+1})^2$. So

$$2Q_k^2 Q_{k+1}^2 + 8P_k^2 P_{k+1}^2 - Q_{2k+1}^2 = (Q_k Q_{k+1} - 2P_k P_{k+1})^2 = (-1)^{2k} = 1,$$

and so the required value of a is established.

On the other hand, from (2.8)

$$Q_k Q_{k+1} = (Q_{2k+1} + (-1)^k)/2, \quad P_k P_{k+1} = (Q_{2k+1} - (-1)^k)/4.$$

Notice that (2.4) is symmetric in x and y. Now, the solution of (2.4) is

$$x = (Q_{2k+1} + 1)/2, \quad y = (Q_{2k+1} - 1)/2, \quad z = P_k^2 + P_{k+1}^2 = P_{2k+1}.$$

So now

$$x^2 + y^2 = \frac{Q_{2k+1}^2 + 1}{2} = P_{2k+1}^2 = z^2,$$

which implies that these solutions also satisfy Equations (2.6). □

By similar arguments, for the equations

$$z^2 = (x^2 + a)^2 - y^2 = x^2 - (y^2 + a)^2, \tag{2.9}$$

the results are as follows.

THEOREM 2.4. *If $a \ge 0$ or the square-free part of $2a + 1$ has a prime divisor of the form $4k + 3$, then Equations (2.9) have no positive integer solutions with $x \ne y$.*

THEOREM 2.5. *If $a = -(Q_{2s}^2 Q_{2t}^2 + 4P_{2s}^2 P_{2t}^2 - 1)/2$, then Equations (2.9) have positive integer solutions*

$$(x, y, z) = (Q_{2s} Q_{2t}, 2P_{2s} P_{2t}, P_{2s}^2 + P_{2t}^2).$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

For equations

$$z^2 = (x^2 + a)^2 - y^2 = x^2 + (y^2 + a)^2, \tag{2.10}$$

we have the following result.

THEOREM 2.6. *Equations (2.10) have no positive integer solution.*

PROOF. From (2.10), we get

$$(x^2 - y^2)(x^2 + y^2 + 2a) = x^2 + y^2.$$

Let $k = x^2 + y^2 + 2a$; then $(k - 1)x^2 = (k + 1)y^2$. This then implies that

$$(k + 1)(k - 1) = k^2 - 1$$

is a square, which is so only for $k = 1$, in which case $y = 0$, contradicting the requirement that $y > 0$. □

Finally, we prove the following theorem.

THEOREM 2.7. *Equations*

$$z^2 = (x^2 + a)^2 + y^2 = x^2 - (y^2 + a)^2$$

have no positive integer solutions with $x \neq y$.

PROOF. In order to prove our theorem let us note that if the equation $(x^2 + a)^2 + y^2 = x^2 - (y^2 + a)^2$ has integer solution (x, y) then a is a root of the quadratic equation (with parameters x and y)

$$2a^2 + 2(x^2 + y^2)a + x^2(x^2 - 1) + y^2(y^2 + 1) = 0.$$

One can see that a is real (not necessarily an integer) if and only if the discriminant

$$\Delta = -4(y^2 - x^2)(y^2 - x^2 + 2) = 4(1 - (y^2 - x^2 + 1)^2) \geq 0,$$

that is,

$$|y^2 - x^2 + 1| \leq 1.$$

Therefore,

$$x^2 - y^2 = 0,\ 1,\ 2.$$

The case $x^2 - y^2 = 0$ contradicts $x \neq y$. If

$$x^2 - y^2 = (x + y)(x - y) = 1,$$

then $x + y = x - y = 1$, so that $y = 0$. If

$$x^2 - y^2 = (x + y)(x - y) = 2,$$

then one of $x \pm y$ is odd and the another is even. This is impossible. □

3. The equation $z^2 = (x^2 + a)^2 - (y^2 + a)^2$

We now consider the Diophantine equation

$$z^2 = (x^2 + a)^2 - (y^2 + a)^2. \tag{3.1}$$

We wish to know for which integer a we can find an integer t such that the above equation has infinitely many solutions in the integers.

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

3.1. Solutions from Pell equations. A simple case is $a = -\tau^2$ for some integer τ. This gives us

$$(z/\tau)^2 = ((x/\tau)^2 - 1)^2 - ((y/\tau)^2 - 1)^2.$$

The following result is more general.

THEOREM 3.1. *If* $2a = (t^2 - 1)r^2 - (t^2 + 1)s^2$ *for some positive integers* t, r, s, *then Equation* (3.1) *has infinitely many solutions in the polynomials* $x(r, s, t)$, $y(r, s, t)$, $z(r, s, t)$.

PROOF. We put $x = tX$, $y = X$, $z = XY(t^2 - 1)$ with $t > 1$. Then for x, y, z defined in this way,

$$0 = z^2 - ((x^2 + a)^2 - (y^2 + a)^2) = X^2(1 - t^2)(2a + (t^2 + 1)X^2 - (t^2 - 1)Y^2).$$

Since x and hence X is a positive integer, we get the Pell equation

$$(t^2 + 1)X^2 - (t^2 - 1)Y^2 = -2a, \tag{3.2}$$

where t a parameter. So when

$$a = ((t^2 - 1)r^2 - (t^2 + 1)s^2)/2, \quad r, s \in \mathbb{Z},$$

Equation (3.2) has a positive integer solution $(X, Y) = (s, r)$. Without loss of generality, we assume that r, s are both positive. By a well-known property of Pell equations, all integer solutions of (3.2) are given by

$$X\sqrt{t^2 + 1} + Y\sqrt{t^2 - 1} = \pm(s\sqrt{t^2 + 1} \pm r\sqrt{t^2 - 1})(t^2 + \sqrt{t^4 - 1})^k, \quad k \in \mathbb{Z}.$$

Thus there exist infinitely many positive solutions $(X, Y) = (X(r, s, t), Y(r, s, t))$ in polynomials

$$\begin{aligned} X_0 &= s, & X_1 &= st^2 + rt^2 - r, & X_{k+2} &= 2t^2X_{k+1} - X_k, \\ Y_0 &= r, & Y_1 &= st^2 + rt^2 + s, & Y_{k+2} &= 2t^2Y_{k+1} - X_k. \end{aligned}$$

Therefore, Equation (3.1) has solutions

$$\begin{aligned} x_0 &= st, & x_1 &= st^3 + rt^3 - rt, & x_{k+2} &= 2t^2x_{k+1} - x_k, \\ y_0 &= s, & y_1 &= st^2 + rt^2 - r, & y_{k+2} &= 2t^2y_{k+1} - y_k, \\ z_0 &= sr(t^2 - 1), & z_1 &= (st^2 + rt^2 - r)(st^2 + rt^2 + s)(t^2 - 1), \\ & & z_{k+2} &= 2t^2z_{k+1} - z_k. \end{aligned}$$

This completes the proof. □

REMARK 3.2. By choosing $s = t = \tau$ in Theorem 3.1, we have $a = -\tau^2$, and Equation (3.1) has solutions with initial terms

$$\begin{aligned} x_1 &= t^2(2t^2 - 1), & x_2 &= t^2(4t^4 - 2t^2 - 1), \\ y_1 &= t(2t^2 - 1), & y_2 &= t(4t^4 - 2t^2 - 1), \\ z_1 &= t^2(4t^4 - 1)(t^2 - 1), & z_2 &= t^2(4t^4 - 2t^2 - 1)(4t^4 + 2t^2 - 1)(t^2 - 1). \end{aligned}$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

3.2. The general case. Let us consider the Pell equation

$$(t^2+1)x^2-(t^2-1)y^2=-2a, \quad a\neq 0. \tag{3.3}$$

Then

$$\begin{aligned}\left|\sqrt{\frac{t^2+1}{t^2-1}}-\frac{y}{x}\right| &= \left|\frac{t^2+1}{t^2-1}-\frac{y^2}{x^2}\right|\cdot\left|\sqrt{\frac{t^2+1}{t^2-1}}+\frac{y}{x}\right|^{-1}\\ &< \left|\frac{2a}{(t^2-1)x^2}\right|\cdot\left|\sqrt{\frac{t^2+1}{t^2-1}}\right|^{-1} < \frac{2a}{\sqrt{t^4-1}x^2}.\end{aligned}$$

Let p_n/q_n denote the nth convergent of a real number α. The following result of Worley [7] and Dujella [1] extends classical results of Legendre and Fatou concerning Diophantine approximations of the form $|\alpha-a/b|<1/(2b^2)$ and $|\alpha-a/b|<1/b^2$.

Let m be the largest odd integer satisfying

$$\alpha<\frac{a}{b}\leq\frac{p_m}{q_m}.$$

Define the numbers r and s by

$$\begin{aligned}a&=rp_{m+1}+sp_m,\\ b&=rq_{m+1}+sq_m.\end{aligned}$$

THEOREM 3.3 (Worley [7], Dujella [1]). *Let α be a real number and a and b co-prime nonzero integers satisfying the inequality*

$$\left|\alpha-\frac{a}{b}\right|<\frac{M}{b^2},$$

where M is a positive real number. Then

$$(a,b)=(rp_{k+1}\pm up_k,\ rq_{k+1}\pm uq_k),$$

for some $k\geq -1$ and nonnegative integers r and u such that $ru<2M$.

The simple continued fraction expansion of a quadratic irrational $\alpha=(a+\sqrt{d})/b$ is periodic. This expansion can be obtained using the following algorithm. Multiplying the numerator and denominator by b, if necessary, we may assume that $b\mid(d-a^2)$. Let $s_0=a$, $t_0=b$ and

$$a_n=\left\lfloor\frac{s_n+\sqrt{d}}{t_n}\right\rfloor,\quad s_{n+1}=a_nt_n-s_n,\quad t_{n+1}=\frac{d-s_{n+1}^2}{t_n}\quad\text{for } n\geq 0. \tag{3.4}$$

If $(s_j,t_j)=(s_k,t_k)$ for $j<k$, then

$$\alpha=[a_0,\ldots,a_{j-1},\overline{a_j,\ldots,a_{k-1}}].$$

We need the following lemma (see Dujella and Jadrijević [2, Lemma 2]).

LEMMA 3.4. *Let $\alpha\beta$ be a positive integer which is not a perfect square, and let p_k/q_k denote the kth convergent of the continued fraction expansion of $\sqrt{\alpha/\beta}$. Let the*

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

sequences (s_k) *and* (t_k) *be defined by* (3.4) *for the quadratic irrational* $\sqrt{\alpha/\beta}$. *Then*

$$\alpha(rq_{k+1} + uq_k)^2 - \beta(rp_{k+1} + up_k)^2 = (-1)^k(u^2 t_{k+1} + 2rus_{k+2} - r^2 t_{k+2}). \quad (3.5)$$

Using the above algorithm, one can check that

$$\sqrt{\frac{t^2+1}{t^2-1}} = [1; \overline{t^2-1, 2}]$$

with

$$(s_0, t_0) = (0, t^2-1), \quad (s_{2k-1}, t_{2k-1}) = (t^2-1, 2), \quad (s_{2k}, t_{2k}) = (t^2-1, t^2-1).$$

Therefore, we get

$$2a = (-1)^k(u^2 t_{k+1} + 2rus_{k+2} - r^2 t_{k+2}).$$

Checking the possibilities (we only need to check $k = -1, 0, 1$),

$$2a = \begin{cases} -((t^2-1)u^2 + 2(t^2-1)ru - 2r^2) & \text{if } k \text{ odd,} \\ 2u^2 + 2ru(t^2-1) - (t^2-1)r^2 & \text{if } k \text{ even,} \end{cases}$$

where $ru < 4|a|/\sqrt{t^4-1}$. Therefore, knowing a convergent p_k/q_k, one can first determine r, u (if there is any) satisfying $ru < 4|a|/\sqrt{t^4-1}$ and then one obtains x, y by

$$x = rq_{k+1} \pm uq_k, \quad y = rp_{k+1} \pm up_k.$$

REMARK 3.5. We firmly believe that for any a the equation $z^2 = (x^2+a)^2 - (y^2+a)^2$ has a nontrivial solution in the integers. Using a simple computer search, we find, for given square-free a, with $|a| < 100$, the smallest integer solution of the equation $z^2 = (x^2+a)^2 - (y^2+a)^2$ satisfying the conditions $0 < y < x$, $z \neq 0$. Our computations are contained in Tables 1 and 2. Up to the time of writing, we have been unable to find any integer solution for the Diophantine equation $z^2 = (x^2+37)^2 - (y^2+37)^2$. This equation has no solutions in the range $0 < y < x < 2 \cdot 10^5$.

3.3. Some particular cases.

In this subsection, we consider some particular values of a and we obtain the following results.

THEOREM 3.6. *If* $a = s^2 - t^2(u^4+v^4)$ *or* $2a = s^2 - t^2(u^4 + 6u^2v^2 + v^4)$, *then Equation* (3.1) *has infinitely many integer solutions with two parameters.*

PROOF. From Equation (3.1),

$$z^2 = (x^2 - y^2)(x^2 + y^2 + 2a).$$

We take

$$x^2 - y^2 = z_1^2, \quad x^2 + y^2 + 2a = z_2^2, \quad z = z_1 z_2. \quad (3.6)$$

The equation $x^2 - y^2 = z_1^2$ has solutions of the form

$$x = t(u^2+v^2), \quad y = t(u^2-v^2), \quad z_1 = 2tuv.$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

TABLE 1. Integer solutions to the Diophantine equation $z^2 = (x^2 + a)^2 - (y^2 + a)^2$, for $a > 0$.

a	x	y	z	a	x	y	z	a	x	y	z
1	5	3	24	34	69	15	4788	69	21	3	504
2	11	5	120	35	2	1	15	70	72	70	1704
3	16	9	245	37				71	2	1	21
5	6	2	40	38	7	5	60	73	85	75	4560
6	8	6	56	39	26	18	616	74	11	1	180
7	29	21	720	41	12	4	176	77	103	97	4920
10	9	5	84	42	25	21	460	78	182	168	17 360
11	2	1	9	43	152	73	22 515	79	9	7	96
13	2445	525	5 971 680	46	10	8	96	82	81	45	6300
14	4	2	24	47	15	9	240	83	18	7	385
15	5	3	32	51	6	3	63	85	54	46	2040
17	153	47	23 320	53	66	34	4240	86	4	2	48
19	4	3	21	55	5	3	48	87	10	1	165
21	22	14	456	57	319	231	86 680	89	12	4	208
22	26	24	360	58	260	240	35 400	91	13	3	240
23	10	2	120	59	3	1	32	93	1346	1246	933 840
26	13	7	180	61	6	2	72	94	10	6	144
29	6	2	56	62	5	1	60	95	3	1	40
30	10	6	112	65	13	5	216	97	409	391	67 920
31	3	1	24	66	20	12	416				
33	5	3	40	67	144	69	20 235				

The second equation of (3.6) implies that

$$2a = z_2^2 - x^2 - y^2 = z_2^2 - 2t^2(u^4 + v^4).$$

So $2 \mid z_2$ and we take $z_2 = 2s$. Therefore $a = s^2 - t^2(u^4 + v^4)$, and so, for this choice of a, the solutions of (3.1) are

$$x = t(u^2 + v^2), \qquad y = t(y^2 - v^2), \qquad z = 4stuv.$$

The equation $x^2 - y^2 = z_1^2$ also has solutions of the form

$$x = t(u^2 + v^2), \qquad y = 2tuv, \qquad z_1 = t(u^2 - v^2),$$

leading to $2a = z_2^2 - t^2(u^4 + 6u^2v^2 + v^4)$. Thus with this value of $2a$,

$$x = t(u^2 + v^2), \qquad y = 2tuv, \qquad z = 2st(u^2 - v^2)$$

are solutions of (3.1). □

In fact, we also get the following result.

THEOREM 3.7. *If $a = r^2 - m^4 - n^4$ for some integers r, m, n, then Equation (3.1) has infinitely many positive integer solutions (x, y, z).*

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

TABLE 2. Integer solutions to the Diophantine equation $z^2 = (x^2 + a)^2 - (y^2 + a)^2$, for $a < 0$.

a	x	y	z	a	x	y	z	a	x	y	z
−1	2	1	3	−34	7	5	12	−69	11	7	48
−2	482	418	153 120	−35	18	14	240	−70	11	5	24
−3	381	69	145 080	−37	14	11	135	−71	12	4	48
−5	10	9	57	−38	476	224	220 920	−73	14	10	120
−6	56	16	3120	−39	93	75	6552	−74	10	8	24
−7	133	35	17 640	−41	9	3	24	−77	125	105	11 040
−10	5	1	12	−42	15	3	180	−78	416	384	90 560
−11	6	2	24	−43	37	13	1320	−79	12	4	16
−13	26	25	255	−46	9	5	28	−82	25	5	540
−14	12	8	120	−47	13	5	120	−83	378	322	98 280
−15	5	3	8	−51	11	3	56	−85	54	46	2040
−17	70	25	4845	−53	27	23	480	−86	19	3	264
−19	6	2	8	−55	12	4	80	−87	25	15	520
−21	6	3	9	−57	17	15	160	−89	13	5	48
−22	15	13	140	−58	29	25	540	−91	13	11	72
−23	630	150	396 240	−59	18	6	264	−93	95	81	6160
−26	13	9	132	−61	9	7	16	−94	12	8	40
−29	8	1	21	−62	40	32	1200	−95	13	5	24
−30	20	12	352	−65	13	5	96	−97	30	25	605
−31	9	1	40	−66	10	6	16				
−33	25	15	560	−67	55	47	2040				

PROOF. From Equation (3.1),

$$x^2 + a = d(r^2 + s^2), \qquad y^2 + a = d(r^2 - s^2), \qquad z = 2drs.$$

Taking $d = 1$ gives $a = r^2 + s^2 - x^2 = r^2 - s^2 - y^2$. It follows that

$$x^2 - y^2 = 2s^2.$$

The above equation yields

$$x = m^2 + 2n^2, \qquad y = |m^2 - 2n^2|, \qquad s = 2mn.$$

Thus, if

$$a = r^2 + s^2 - x^2 = r^2 + (2mn)^2 - (m^2 + 2n^2)^2 = r^2 - m^4 - 4n^4,$$

then Equation (3.1) has the solutions

$$x = m^2 + 2n^2, \qquad y = |m^2 - 2n^2|, \qquad z = 4rmn. \tag{3.7}$$

This concludes the proof. □

4. Equations in triangular and tetrahedral numbers

4.1. On triangular numbers. We start with the problem related to the construction of right triangles with legs which are triangular numbers. Thus, we will be interested in integer solutions of the Diophantine equation

$$z^2 = t_x^2 + t_y^2. \tag{4.1}$$

Sierpiński in [4, p. 34] has shown that the above equation has infinitely many solutions in the integers. However, all solutions presented by him satisfied the condition $\mathrm{GCD}(t_x, t_y) > 1$. In other words, the triple $X = t_x$, $Y = t_y$, $Z = z$ which satisfies the equation $X^2 + Y^2 = Z^2$ is not a primitive solution. As pointed out by Sierpiński [4, p. 35], personal communication with A. Schinzel showed that the set of integer solutions of Equation (4.1) which satisfy the condition $\mathrm{GCD}(t_x, t_y) = 1$ is infinite. However, the solution obtained by Schinzel is not parametric. It is natural to ask whether Equation (4.1) has parametric solutions. In other words: does Equation (4.1) have solutions in the ring $\mathbb{Z}[u]$?

Generally, these questions are very difficult and we do not have any general theory that can be used. However, as we will see, for our particular equation it is possible to construct infinitely many polynomials $x(u), y(u), z(u) \in \mathbb{Z}[u]$ that satisfy the condition $\mathrm{GCD}(t_{x(u)}, t_{y(u)}) = 1$.

It is clear that we can consider the equation

$$z^2 = (x^2 - 1)^2 + (y^2 - 1)^2.$$

Indeed, if the triple $(x, y, z) = (p, q, r)$ satisfies the above equation, then the triple $(2p + 1, 2q + 1, 8r)$ satisfies the equation $z^2 = t_x^2 + t_y^2$. We then deduce that $x^2 - 1$, $y^2 - 1$, z must be a solution of Pythagoras's equation $X^2 + Y^2 = Z^2$. It is well known that all solutions of this equation are of the form

$$X = 2dst, \quad Y = d(s^2 - t^2), \quad Z = d(s^2 + t^2),$$

where s, t, d are certain integers. Let us put $d = 1$ and consider the system of equations given by

$$x^2 = 2st + 1, \quad y^2 = s^2 - t^2 + 1.$$

The first equation of the above system is satisfied if we put

$$s = 2u(ku - 1), \quad t = k, \quad x = 2ku - 1.$$

Putting the above quantities into the equation $y^2 = s^2 - t^2 + 1$ yields

$$y^2 = (4u^4 - 1)k^2 - 8u^3k + 4u^2 + 1 =: f(k).$$

This is a Pell equation depending on the parameter u. Let us note that $f(1) = (2u(u - 1))^2$ and that the following identity holds:

$$\begin{aligned} f((8u^4 - 1)k + 4u^2y - 8u^3) - (4u^2(4u^4 - 1)k + (8u^4 - 1)y - 16u^5)^2 \\ = f(k) - y^2. \end{aligned}$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

From the above we can deduce that if we define

$$\begin{aligned} k_0 &= 1, \quad y_0 = 2u(u-1), \\ k_n &= (8u^4-1)k_{n-1} + 4u^2 y_{n-1} - u^3, \\ y_n &= 4u^2(4u^4-1)k_{n-1} + (8u^4-1)y_{n-1} - 16u^5, \end{aligned} \tag{4.2}$$

then the polynomials

$$p_n(u) = k_n(u)u - 1, \quad q_n(u), \quad r_n(u) = u^2(uk_n(u)-2)^2/4 + k_n(u)^2$$

for $n = 1, 2, \ldots$, satisfy the equation

$$(p^2-1)^2 + (q^2-1)^2 = r^2.$$

Finally, the polynomials

$$x_n(u) = (p_n(u)-1)/2, \quad y_n(u) = (q_n(u)-1)/2, \quad z_n(u) = r_n(u)/8$$

satisfy the equation $t_x^2 + t_y^2 = z^2$. In particular, for $n = 1$ we get

$$\begin{aligned} x_1(u) &= (u^5 - 2u^4 - u - 2)/2, \\ y_1(u) &= (u^2+1)(u^4 - 2u^3 - u^2 + 2u - 2)/4, \\ z_1(u) &= (u^{12} - 4u^{11} + 4u^{10} + 2u^8 - 16u^7 + 24u^6 - 7u^4 + 20u^3 + 4u^2 + 4)/32. \end{aligned}$$

The resultant $\mathrm{Res}(t_{x_1}, t_{y_1})$ of the polynomials $t_{x_1(u)}, t_{y_1(u)}$ is equal to 2^{-58}. This means that the polynomials are co-prime. Let us note that the polynomials $x_n(2u+1)$, $y_n(2u+1)$, $z_n(2u+1)$ belong to $\mathbb{Z}[u]$. It is possible to prove (we will not do this here) that for each positive integer n the polynomials $t_{x_n(u)}, t_{y_n(u)}$ are co-prime. We have proved the following result.

THEOREM 4.1. *The equation $z^2 = t_x^2 + t_y^2$ has infinitely many solutions in polynomials $x(u), y(u), z(u) \in \mathbb{Z}[u]$ that satisfy the condition* $\mathrm{GCD}(t_{x(u)}, t_{y(u)}) = 1$.

We deduce the following corollary.

COROLLARY 4.2. *Let $a, b \in \mathbb{N}_+$ and $f(x) = (x+a)(x+b)$. The Diophantine equation $z^2 = f(x)^2 + f(y)^2$ has infinitely many polynomial solutions.*

PROOF. Let us take $b' \in \mathbb{Z} \setminus \{0\}$. Note that if the triple $(x(u), y(u), z(u))$ is a solution of the equation $z^2 = t_x^2 + t_y^2$, then the triple $(b'x(u), b'y(u), 2b'^2 z(u))$ is a solution of the equation

$$z^2 = (x(x+b'))^2 + (y(y+b'))^2.$$

Putting $b' = b - a$, we deduce that the triple

$$((b-a)x(u) + a, (b-a)y(u) + a, 2(b-a)^2 z(u))$$

is a solution of the Diophantine equation

$$z^2 = ((x+a)(x+b))^2 + ((y+a)(y+b))^2.$$

This proves the corollary. □

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

Numerical investigations suggests the following conjecture.

CONJECTURE 4.3. Let us consider the rational numbers

$$R_n = \text{Discriminant}(t_{x_n(u)}, t_{y_n(u)}).$$

Then $R_n = 2^{-40n-18}$.

REMARK 4.4. The problem of construction of the right-angled triangles for which all sides are triangular numbers, $t_x^2 + t_y^2 = t_z^2$, was posed by K. Zarankiewicz (see [4, p. 34]). Only one integer solution of this equation is known so far: $x = 132$, $y = 143$, $z = 164$. We tried to use the parametric solutions of the equation $z^2 = t_x^2 + t_y^2$ to find other integers satisfying the Zarankiewicz equation, but without success.

We conclude this subsection with an interesting theorem.

THEOREM 4.5. *Let us take $n \in \mathbb{N}_+$. Then the Diophantine equation $z^2 = x^n + t_y^2$ has infinitely many positive integer solutions.*

PROOF. If we take

$$x = u^{12}, \quad y = u^{4n} - 1, \quad z = \frac{u^{4n}(u^{4n}+1)}{2},$$

then $z^2 = x^n + t_y^2$ and our theorem is proved. □

4.2. On tetrahedral numbers. In this subsection, we will consider the problem of construction of right-angled triangles with legs that are tetrahedral numbers. Thus, we are interested in the integer solutions of the Diophantine equation

$$z^2 = T_x^2 + T_y^2. \tag{4.3}$$

Let us note that $91^2 = T_5^2 + T_7^2$, so this equation has an integer solution. Sierpiński in [4, p. 57] wrote that it is unclear whether Equation (4.3) has infinitely many solutions in the integers. However, without much trouble we can construct infinitely many solutions of this equation which satisfy the condition $y - x = 1$. Indeed, we have

$$T_{6x}^2 + T_{6x+1}^2 = (3x+1)^2(6x+1)^2 g(x),$$

where $g(x) = 8x^2 + 4x + 1$. Because $g(0) = 1$ and the identity

$$g(17x + 6z + 4) - (48x + 17z + 12)^2 = g(x) - z^2,$$

holds, we can see that the equation $g(x) = z^2$ has infinitely many solutions x_n, z_n given by

$$x_0 = 0, \quad z_0 = 1, \quad x_n = 17x_{n-1} + 6z_{n-1} + 4, \quad z_n = 48x_{n-1} + 17z_{n-1} + 12.$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

From the above, for each n, we get the identity

$$((3x_n+1)(6x_n+1)z_n)^2 = T_{6x_n}^2 + T_{6x_n+1}^2.$$

In particular

$$T_{60}^2 + T_{61}^2 = 54\,839^2, \quad T_{2088}^2 + T_{2089}^2 = 2\,150\,259\,925^2, \ldots .$$

In the light of the above result, it is interesting to ask whether it is possible to find an infinite family of solutions x_n, y_n, z_n of Equation (4.3) such that $y_n - x_n \to \infty$.

We will construct two families that satisfy this condition. We are looking for the solutions of Equation (4.3) of the following form

$$\begin{aligned} x &= x(u, v) = v^2 - u^2 - 1, \\ y &= y(u, v) = \frac{3v^2 - 2uv + 3u^2 - 3}{2}, \\ z &= z(u, v) = \frac{(v^2 - u^2)Z(u, v)}{192}, \end{aligned} \tag{4.4}$$

where u, v have opposite parity and

$$\begin{aligned} Z(u, v) = {} & 105v^4 - 108uv^3 + (150u^2 - 96)v^2 \\ & - 4u(27u^2 - 16)v + 3(u^2 - 1)(35u^2 + 3). \end{aligned}$$

For x, y, z defined above we have the identity

$$T_{x(u,v)}^2 + T_{y(u,v)}^2 - z(u, v)^2 = \frac{h(u, v)(h(u, v) + 2)H(u, v)}{36\,864},$$

where

$$h(u, v) = -1 + u^2 - 6uv + v^2$$

and

$$H(u, v) = 1663v^8 - 4020uv^7 + \cdots + 288u^2 - 144$$

is a polynomial of degree eight. We omit the full expansion of the polynomial H since it is not necessary for our purposes. From this identity we deduce that

$$T_{x(u,v)}^2 + T_{y(u,v)}^2 - z(u, v)^2 = 0$$

if and only if $h(u, v) = 0$, or $h(u, v) + 2 = 0$, or $H(u, v) = 0$.

We show that the equation $h(u, v) = 0$ has infinitely many solutions in the positive integers u, v. From the equation $h(u, v) = 0$, it is clear that if the pair u, v is a solution then the numbers u, v are of different parity and for each such pair the number $y(u, v)$ is an integer, and the same holds for $z(u, v)$.

In order to show that $h(u, v) = 0$ has infinitely many solutions in the integers we note the identity

$$h(u, v) = h(v, 6v - u).$$

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

Now from the equality $h(6, 35) = 0$ and the above identity we deduce that

$$0 = h(6, 35) = h(35, 6 \cdot 35 - 6) = 0,$$

and more generally, if we define the sequences $\{u_n\}_{n=0}^{\infty}$, $\{v_n\}_{n=0}^{\infty}$ recursively by

$$u_0 = 6, \quad v_0 = 35, \quad u_n = v_{n-1}, \quad v_n = 6v_{n-1} - u_{n-1}, \quad \text{for } n \geq 1,$$

then $h(u_n, v_n) = 0$ for each $n \in \mathbb{N}$. Therefore, we conclude that the numbers

$$x = x(u_n, v_n), \quad y = y(u_n, v_n), \quad z = z(u_n, v_n)$$

are integer solutions of the Diophantine equation $T_x^2 + T_y^2 = z^2$. In particular, for $n = 0$ we get

$$T_{1188}^2 + T_{1680}^2 = 839\,790\,700^2,$$

and for $n = 1$ we get

$$T_{40390}^2 + T_{57120}^2 = 32\,946\,833\,683\,400^2.$$

In order to give the second family of solutions we define

$$x'(u, v) = x(u, v),$$
$$y'(u, v) = y(u, v) + 1,$$
$$z'(u, v) = \frac{(v^2 - u^2)Z'(u, v)}{192},$$

where

$$Z'(u, v) = 105v^4 - 108uv^3 + (150u^2 + 96)v^2 - 4u(27u^2 + 16)v + 3(u^2 + 1)(35u^2 - 3)$$

and $x(u, v)$, $y(u, v)$ are defined by (4.4). For x', y', z' defined above, we have an identity

$$T_{x'(u,v)}^2 + T_{y'(u,v)}^2 - z'(u, v)^2 = \frac{h(u, v)(h(u, v) + 2)H'(u, v)}{36\,864},$$

where $h(u, v)$ is the same polynomial we obtained previously and H' is a polynomial of degree eight. By the same method, one can show that the numbers

$$x' = x(u_n, v_n), \quad y' = y(u_n, v_n) + 1, \quad z' = z'(u_n, v_n)$$

are integer solutions of the Diophantine equation $T_x^2 + T_y^2 = z^2$.

Let us note that in fact our reasoning implies that the set of integer solutions of the system of equations

$$z_1^2 = T_x^2 + T_y^2, \quad z_2^2 = T_x^2 + T_{y+1}^2$$

is infinite. These results are quite unexpected and the following natural problem arises.

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

PROBLEM 4.6. Find integer-valued polynomials $f \in \mathbb{Q}[X]$ with the property that the set of integer solutions of the system of equations

$$z_1^2 = f(x)^2 + f(y)^2, \quad z_2^2 = f(x)^2 + f(y+1)^2$$

is infinite.

Let us gather together what we have proved in the following theorem.

THEOREM 4.7.

(1) *The equation* $T_x^2 + T_y^2 = z^2$ *has infinitely many integer solutions satisfying the condition* $y - x = 1$.

(2) *There exists an infinite sequence of solutions* (x_n, y_n, z_n) *of the equation*

$$T_x^2 + T_y^2 = z^2$$

such that $y_n - x_n \to \infty$.

(3) *The set of integer solutions of the system of equations*

$$z_1^2 = T_x^2 + T_y^2, \quad z_2^2 = T_x^2 + T_{y+1}^2$$

is infinite.

For the families of solutions of Equation (4.3) that we obtained, T_x and T_y are not co-prime. Thus, it is natural to ask the following question.

PROBLEM 4.8. Does the equation $z^2 = T_x^2 + T_y^2$ have infinitely many solutions in integers x, y, z that satisfy the condition $\mathrm{GCD}(T_x, T_y) = 1$?

In the range $x < y < 10^5$ there are exactly 39 solutions of our equation, but only one solution, given by

$$x = 143, \quad y = 237, \quad z = 2\,301\,289,$$

that satisfies the condition $\mathrm{GCD}(T_x, T_y) = 1$.

Acknowledgements

The authors express their gratitude to the anonymous referee for constructive suggestions to improve an earlier draft of this paper. They are also grateful to Professor A. Schinzel for useful comments.

References

[1] A. Dujella, 'Continued fractions and RSA with small secret exponent', *Tatra Mt. Math. Publ.* **29** (2004), 101–112.

[2] A. Dujella and B. Jadrijević, 'A family of quartic Thue inequations', *Acta Arith.* **111** (2004), 61–76.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edn (Clarendon Press, Oxford, 1960).

[4] W. Sierpiński, *Triangular Numbers*, Biblioteczka Matematyczna, 12 (PZWS, Warsaw, 1962) (in Polish).

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press

[5] M. Ulas, 'On the Diophantine equation $f(x)f(y) = f(z)^2$', *Colloq. Math.* **107** (2007), 1–6.

[6] M. Ulas and A. Togbé, 'On the Diophantine equation $z^2 = f(x)^2 \pm f(y)^2$', *Publ. Math. Debrecen* **76**(1–2) (2010), 183–201.

[7] R. T. Worley, 'Estimating $|\alpha - p/q|$', *J. Aust. Math. Soc.* **31** (1981), 202–206.

BO HE, Department of Mathematics, ABa Teacher's College, Wenchuan,
Sichuan 623000, PR China
e-mail: bhe@live.cn

ALAIN TOGBÉ, Mathematics Department, Purdue University North Central,
1401 S, U.S. 421, Westville IN 46391, USA
e-mail: atogbe@pnc.edu

MACIEJ ULAS, Institute of Mathematics, Jagiellonian University, Łojasiewicza 6,
30-348 Kraków, Poland
and
Institute of Mathematics, Polish Academy of Sciences, Śniadeckich 8,
00-956 Warszawa, Poland
e-mail: Maciej.Ulas@im.uj.edu.pl

https://doi.org/10.1017/S0004972710000377 Published online by Cambridge University Press