A NOTE ON A CONJECTURE OF JEŠMANOWICZ

BY

MOUJIE DENG (A CHENG CITY)
AND G. L. COHEN (BROADWAY, NSW)

Abstract. Let $a$, $b$, $c$ be relatively prime positive integers such that $a^2 + b^2 = c^2$. Ješmanowicz conjectured in 1956 that for any given positive integer $n$ the only solution of $(an)^x + (bn)^y = (cn)^z$ in positive integers is $x = y = z = 2$. If $n = 1$, then, equivalently, the equation $(u^2 - v^2)^x + (2uv)^y = (u^2 + v^2)^z$, for integers $u > v > 0$, has only the solution $x = y = z = 2$. We prove that this is the case when one of $u$, $v$ has no prime factor of the form $4l + 1$ and certain congruence and inequality conditions on $u$, $v$ are satisfied.

1. Introduction. Let $a$, $b$, $c$ be relatively prime positive integers such that $a^2 + b^2 = c^2$, and let $n$ be a positive integer. Then the Diophantine equation

$$(na)^x + (nb)^y = (nc)^z$$

has solution $x = y = z = 2$. Ješmanowicz [4] conjectured in 1956 that there are no other solutions of (1). Building on the work of Dem’yanenko [2], we proved in [3] that the conjecture is true when $n > 1$, $c = b + 1$ and certain further divisibility conditions are satisfied.

If $n = 1$, (1) is equivalent to

$$(u^2 - v^2)^x + (2uv)^y = (u^2 + v^2)^z,$$

where $u$, $v$ are integers such that $u > v > 0$, gcd$(u, v) = 1$, and one of $u$, $v$ is even, the other odd. A number of special cases of Ješmanowicz’s conjecture have been settled. Sierpiński [8] and Ješmanowicz [4] proved it for $(u, v) = (2, 1)$ and $(u, v) = (3, 2), (4, 3), (5, 4)$ and $(6, 5)$, respectively. Lu [7] proved it when $v = 1$, and Dem’yanenko [2] when $v = u - 1$. Takakuwa [9] proved the conjecture in a number of special cases in which, in particular, $v$ ≡ 1 (mod 4), and, in [10], when $u$ is exactly divisible by 2 and $v = 3, 7, 11$ or 15. Le [6] proved it when $uv$ is exactly divisible by 2, $v$ ≡ 3 (mod 4) and $u ≥ 81v$. Chao Ko [5] and Jingrun Chen [1] proved the conjecture when $uv$ has no prime factor of the form $4l + 1$ and certain congruence and inequality conditions on $u$, $v$ are satisfied.

2000 Mathematics Subject Classification: 11D61.
In this note, we shall prove that the conjecture is true if one of \( u, v \) has no prime factor of the form \( 4l + 1 \), and certain congruence and inequality conditions on \( u, v \) are satisfied.

2. Main results

**Theorem 1.** Suppose \( u \) is even with no prime factor of the form \( 4l + 1 \), \( u > v > 0 \) and \( \gcd(u, v) = 1 \). Write \( u = 2m \) and suppose also that one of the following is true:

(i) \( m \equiv 1 \pmod{2}, v \equiv 1 \pmod{4}, u^2 - v^2 \) has a prime factor of the form \( 8l + 5 \) or \( u - v \) has a prime factor of the form \( 8l + 3 \);

(ii) \( m \equiv 1 \pmod{2}, v \equiv 3 \pmod{4}, u + v \) has a prime factor of the form \( 8l + 3 \);

(iii) \( m \equiv 2 \pmod{4}, v \equiv 3, 7 \pmod{8} \);

(iv) \( m \equiv 2 \pmod{4}, v \equiv 5 \pmod{8}, u + v \) has a prime factor of the form \( 8l + 7 \);

(v) \( m \equiv 2 \pmod{4}, v \equiv 1 \pmod{8}, u + v \) has a prime factor of the form \( 8l + 3 \);

(vi) \( m \equiv 0 \pmod{4}, v \equiv 1 \pmod{8}, u + v \) has a prime factor of the form \( 8l + 3 \), \( u^2 - v^2 \) has a prime factor of the form \( 8l + 5 \) or \( u - v \) has a prime factor of the form \( 8l + 3 \);

(vii) \( m \equiv 0 \pmod{4}, v \equiv 3, 5 \pmod{8} \);

(viii) \( m \equiv 0 \pmod{4}, v \equiv 7 \pmod{8}, u^2 - v^2 \) has a prime factor of the form \( 8l + 3 \) or \( 8l + 5 \).

Then the Diophantine equation (2) has no positive integer solution other than \( x = y = z = 2 \).

**Proof.** Modulo 4, (2) becomes \((-1)^x \equiv 1\), so \( x \) is even. We now show that \( z \) is also even, and that, except perhaps in case (ii), \( y \) is even.

The following simple congruences are required:

\[
2uv \equiv 2v^2 \pmod{u - v}, \quad u^2 + v^2 \equiv 2v^2 \pmod{u - v},
\]

\[
2uv \equiv -2v^2 \pmod{u + v}, \quad u^2 + v^2 \equiv 2v^2 \pmod{u + v}.
\]

In case (i), we have \( 2m + v \equiv 3 \pmod{4} \), so \( u + v \) has either a prime factor, \( p \) say, of the form \( 8l + 3 \), or a prime factor, \( q \) say, of the form \( 8l + 7 \) (or both). In the former case, from (2) and (3),

\[
(-2v^2)^y \equiv (2v^2)^z \pmod{p},
\]

and it follows that

\[
1 = \left( \frac{-2}{p} \right)^y = \left( \frac{-2v^2}{p} \right)^y = \left( \frac{(-2v^2)^y}{p} \right) = \left( \frac{(2v^2)^z}{p} \right)^z = \left( \frac{2}{p} \right)^z = (-1)^z,
\]
where $(\cdot)$ is Legendre’s symbol. So $z$ is even. In the latter case, we find in the same way that $y$ is even.

If $v^2 - u^2$ has a prime factor of the form $8l + 5$, or $u - v$ has a prime factor of the form $8l + 3$, then, again in the same way, we find that $y \equiv z \pmod{2}$. Then $y$ and $z$ are even in case (i), and we may similarly obtain the same conclusion in cases (vi) and (viii).

In case (ii), since $u + v$ has a prime factor of the form $8l + 3$ or $8l + 7$, we find as above that $z$ is even or $y$ is even. If $y$ is even, then $y > 1$, and, recalling that $x$ is even, from (2) we have $5^2 \equiv 1 \pmod{8}$. It follows that, in case (ii), $z$ must be even.

Consider case (iii). If $v \equiv 3 \pmod{8}$, then $u + v \equiv 7 \pmod{8}$. From (2) and (3), we have $-2v^2 \equiv (2v^2)^z \pmod{u + v}$, so that

$$(-1)^y = \left(\frac{-2v^2}{u + v}\right)^y = \left(\frac{2v^2}{u + v}\right)^z = 1,$$

where $(\cdot)$ is Jacobi’s symbol. Then $y$ is even. From (2), $1 \equiv 9^z \pmod{16}$, which implies $z$ is even. If $v \equiv 7 \pmod{8}$, then, considering (2) modulo $u + v$ and $u - v$, respectively, we may similarly show that $y$ and $z$ are even. This also follows in a similar fashion in cases (iv), (v) and (vii).

In all cases except one, we have now shown that $y$ and $z$ are both even. The exception is case (ii), in which we know only that $z$ is even. We show now that $y$ must be even in this case as well.

Write $x = 2x_1$ and $z = 2z_1$. Then, from (2),

$$(4mv)^y = ((4m^2 + v^2)^{z_1} + (4m^2 - v^2)^{z_1})(4m^2 + v^2)^{z_1} - (4m^2 - v^2)^{z_1}).$$

If $x_1$ is even, then $(4m^2 + v^2)^{z_1} + (4m^2 - v^2)^{z_1} \equiv 2 \pmod{4}$. Let $p$ be an odd prime factor of $m$, so that, by hypothesis, $p \equiv 3 \pmod{4}$. Since $\gcd(m, v) = 1$, and since $-1$ is a quadratic nonresidue of $p$, we have

$$4m^2 + v^2 \equiv (4m^2 - v^2)^{z_1} \equiv v^{2z_1} + v^{2x_1} \not\equiv 0 \pmod{p},$$

It follows that

$$4m^2 + v^2 \equiv (4m^2 - v^2)^{z_1} = 2v_1^y,$$

and,

$$(4m^2 + v^2)^{z_1} - (4m^2 - v^2)^{z_1} = 2^{2y-1}m^y v_2^y,$$

where $v = v_1 v_2$. We will show that $v_2 > 1$. In case (ii), $v \equiv 3 \pmod{4}$, so $v$ has a prime factor $q \equiv 3 \pmod{4}$ and, as in (4),

$$(4m^2 + v^2)^{z_1} + (4m^2 - v^2)^{z_1} \equiv (2m)^{2x_1} + (2m)^{2z_1} \not\equiv 0 \pmod{q}.$$
where \( v = v_3v_4 \), so that
\[(4m^2 + v^2)x_1 - (4m^2 - v^2)x_1 = 2v_4^y,\]
where \( v = v_3v_4 \), so that
\[(7) \quad (4m^2 + v^2)x_1 = 2^{2y-2}m^y v_3^y + v_4^y,\]
\[(8) \quad (4m^2 - v^2)x_1 = 2^{2y-2}m^y v_3^y - v_4^y.\]
From (7), \( \gcd(v_3, v_4) = 1 \), \( y > 1 \) and \( v_2^{2z_1} \equiv v_4^y \quad (\text{mod} \ 4) \). But, in case (ii), as shown above for \( v_2 \), we have \( v_4 = 3 \mod 4 \), \( 3 \equiv 3^y \mod 4 \), and it follows that \( y \) is even, as required.

We now complete the proof of Theorem 1.

Notice first that \( x_1 \) must be odd. To confirm this, consider again the passage above in which it was assumed that \( x_1 \) is even. Then, since \( y \geq 2 \), it follows that \( 2^{2y-1}m^y v_3^y \geq 2^{y-1}(2m)^y > 2^{y-1}v_3^y \geq 2v_3^y \), so, again, (5) and (6) cannot both hold. With \( x_1 \) odd, we may refer again to (7) and (8).

Write \( y = 2y_1 \). From (8),
\[(4m^2 - v^2)x_1 = (2^{2y-1}m^y v_3^{y_1} + v_4^{y_1})(2^{2y-1}m^y v_3^{y_1} - v_4^{y_1}).\]
Since \( \gcd(v_3, v_4) = 1 \), the factors on the right are relatively prime. Let \( 2^{2y-1}m^y v_3^{y_1} + v_4^{y_1} = x_1 \) and \( 2^{2y-1}m^y v_3^{y_1} - v_4^{y_1} = t x_1 \). Then
\[(9) \quad st = 4m^2 - v^2, \quad \gcd(s, t) = 1, \ s \geq t + 2.\]
We have
\[s^{x_1} + t^{x_1} = 2^{y_1}(2m)^{y_1}v_3^{y_1} > 2^{y_1}v_3^{y_1}v_4^{y_1} = 2^{y_1}v_3^{y_1}v_4^{y_1} = 2^{y_1}v_3^{y_1}v_4^{y_1} (s^{x_1} - t^{x_1}),\]
from which
\[(2^{y_1-1}v_3^{2y_1} + 1)t^{x_1} > (2^{y_1-1}v_3^{2y_1} - 1)s^{x_1} \geq (2^{y_1-1}v_3^{2y_1} - 1)(t + 2)^{x_1} \geq (2^{y_1-1}v_3^{2y_1} - 1)t^{x_1} + 2(2^{y_1-1}v_3^{2y_1} - 1)x_1 t^{x_1-1}.\]
It follows that
\[(10) \quad t > (2^{y_1-1}v_3^{2y_1} - 1)x_1 \geq 2^{y_1-1}v_3^{2y_1} - 1.\]
But, from (8), we have
\[0 \equiv (4m^2 - v^2)x_1 = 2^{2y-2}(2m)^y v_3^y - v_4^y = 2^{2(y_1-1)}(4m^2)v_3^{2y_1} - v_4^{2y_1} \equiv 2^{2(y_1-1)}v_3^{2y_1} - v_4^{2y_1} \quad (\text{mod} \ 4m^2 - v^2),\]
so that \( v_3^{2y}(2^{2(y_1-1)}v_3^{2y_1} - 1) \equiv 0 \quad (\text{mod} \ st) \), by (9). Since \( \gcd(v_4, st) = 1 \), we have \( 2^{2(y_1-1)}v_3^{2y_1} - 1 \equiv 0 \quad (\text{mod} \ st) \). If \( v_3 > 1 \) or \( y_1 > 1 \), then the left-hand side is positive, and we must have \( t^2 < st \leq 2^{2(y_1-1)}v_3^{2y_1} - 1 \), so that \( t \leq 2^{y_1-1}v_3^{2y_1} - 1 \), contradicting (10).

Hence \( v_3 = y_1 = 1 \), and, from (7), \( x_1 = z_1 = 1 \). Thus \( x = y = z = 2 \), completing the proof of Theorem 1.

**Theorem 2.** Suppose \( u \) is even, \( 25v > 2u > 2v > 0 \), \( \gcd(u, v) = 1 \) and \( v \) has no prime factor of the form \( 4l + 1 \). Write \( u = 2m \) and suppose also
that one of conditions (i)–(viii) in Theorem 1 is true. Then the Diophantine equation (2) has no positive integer solution other than \(x = y = z = 2\).

Proof. When one of conditions (i)–(viii) in the statement of Theorem 1 is satisfied, we may show, as in the proof of Theorem 1, that \(x\) and \(z\) are even, and, except in case (ii), \(y\) is even. We show first that \(y\) is even in this case as well. Let \(x = 2x_1\) and \(z = 2z_1\). In much the same way as before, we may show that \(x_1\) is odd and

\[
(4m^2 + v^2)x_1 + (4m^2 - v^2)x_1 = 2^{2y-1}m_1^y,
\]

\[
(4m^2 + v^2)x_1 - (4m^2 - v^2)x_1 = 2m_2^y v^y,
\]

where \(m = m_1 m_2\) and \(m_2 \equiv 1 \pmod{4}\). We have

\[
(4m^2 + v^2)x_1 = 2^{2y-2}m_1^y + m_2^y v^y,
\]

\[
(4m^2 - v^2)x_1 = 2^{2y-2}m_1^y - m_2^y v^y.
\]

From (11), \(y > 1\) so that, in case (ii), \(1 \equiv 3^y \pmod{4}\). Hence \(y\) is even.

Let \(y = 2y_1\). From (12),

\[
(4m^2 - v^2)x_1 = (2^{2y_1-1}m_1^{y_1} + m_2^{y_1} v^{y_1})(2^{2y_1-1}m_1^{y_1} - m_2^{y_1} v^{y_1}).
\]

As in the corresponding part of the proof of Theorem 1, we may put

\[
2^{2y_1-1}m_1^{y_1} + m_2^{y_1} v^{y_1} = s^{x_1}\quad\text{and}\quad 2^{2y_1-1}m_1^{y_1} - m_2^{y_1} v^{y_1} = t^{x_1},
\]

so that

\[
st = 4m^2 - v^2,\quad \gcd(s, t) = 1,\quad s \geq t + 2
\]

and

\[
s^{x_1} + t^{x_1} = 2^{2y_1} m_1^{y_1},\quad s^{x_1} - t^{x_1} = 2m_2^{y_1} v^{y_1}.
\]

If \(m_2 \neq 1\), then \(m_2 \geq 5\). From (14), \((4m_1)^{y_1} > 2(m_2 v)^{y_1}\), so \(4m_1 > m_2 v\). Then \(4m > m_2 v \geq 25v\), contradicting the hypothesis that \(2u < 25v\). Thus, \(m_2 = 1\), and if \(y_1 > 1\) then we may use (13) and (14) to obtain a contradiction, much as in the closing part of the proof of Theorem 1, by showing both \(t \geq 2^{y_1-1}v\) and \(t < 2^{y_1-1}\).

Hence \(m_2 = y_1 = 1\), and it follows from (11) and (12) that \(x_1 = z_1 = 1\). Therefore, \(x = y = z = 2\), completing the proof of Theorem 2.

REFERENCES


Heilongjiang Nongken Teachers’ College
A Cheng City
People’s Republic of China

School of Mathematical Sciences
University of Technology, Sydney
PO Box 123
Broadway, NSW 2007
Australia
E-mail: glc@maths.uts.edu.au

Received 14 May 1999