ON THE DIOPHANTINE EQUATION $x^{2p} + y^{2p} = z^p$

by

A. ROTKIEWICZ (WARSZAWA)

It was shown by Terjanian [12] that if $p$ is an odd prime and $x, y, z$ are positive integers such that $x^{2p} + y^{2p} = z^{2p}$ then $2p$ divides $x$ or $y$. From the theorem of Terjanian the present author [9] deduced that if $x^{2p} + y^{2p} = z^{2p}$ then either $8p^3 | x$ or $8p^3 | y$.

In [10] the impossibility of the diophantine equation $x^p + y^p = z^2$ was established under the conditions $(x, y) = 1$, and either $p | z$, $2 \nmid z$, or $p \nmid z$, $2 | z$ ($p$ prime $> 3$) ([10], Theorem T).

In a joint paper with A. Schinzel [11] we proved that if $x, y, z$ are positive integers such that $x^{2p} + y^{2p} = z^{2p}$ where $p$ is a prime greater than 3 then either $4p^2 | x$ or $4p^2 | y$, and if $x^p + y^{2p} = z^2$ where $x, y$ and $z$ are non-zero integers then $p < 2|y|$, $|x| < 8y^{2p+2}$, which extends Terjanian’s result [14]: if $x^p + y^{2p} = z^2$ then either $2p | x$ or $2p | y$, as well as Chao Ko’s result [2], [3]: the equation $x^p + 1 = z^2$ has no solutions in positive integers if $p$ is a prime greater than 3.

Here we shall prove the following.

THEOREM 1. If $(x, y) = 1$, $p$ is an odd prime and

$$x^{2p} + y^{2p} = z^p$$

then either $4p^2 | x$ or $4p^2 | y$, and there exist coprime positive integers $\alpha$ and $\beta$ such that

$$z = \alpha^{2p} + \frac{\beta^{2p}}{p^2} \quad \text{where } 4p^2 | \beta \text{ and } \alpha^{p-1} \equiv 1 \pmod{p^2},$$

$$x^p = (\alpha^p)^p - \left(\frac{p}{2}\right)(\alpha^p)^{p-2} \left(\frac{\beta}{p}\right)^2 + \left(\frac{p}{4}\right)(\alpha^p)^{p-4} \left(\frac{\beta}{p}\right)^4 - \ldots,$$

$$y^p = \left(\frac{p}{1}\right)(\alpha^p)^{p-1} \left(\frac{\beta}{p}\right) - \left(\frac{p}{3}\right)(\alpha^p)^{p-3} \left(\frac{\beta}{p}\right)^3$$

$$+ \left(\frac{p}{5}\right)(\alpha^p)^{p-5} \left(\frac{\beta}{p}\right)^5 - \ldots$$
Proof. Let \( x^{2p} + y^{2p} = z^p \). If \( 2 \nmid xy \) then \( x^{2p} + y^{2p} \equiv 2 \pmod{4} \), which is impossible. Without loss of generality we can assume that \( 2 \mid y \). We have 
\[
(y^2)^2 = z^p + (-x^2)^p x
\]
and by Theorem T of [10] we have \( p \mid y^p \), hence \( p \mid y \). Since \( (x^2)^p + (y^2)^p + (-z)^p = 0 \), a theorem of Vandiver ([6], p. 327, Theorem 1046) shows that \( (y^2)^p \equiv y^2 \pmod{p^3} \). Since \( p \mid y \), \( p \geq 3 \), we have \( p^3 \mid y^2 \), hence \( p^2 \mid y \).

Now we shall prove that \( 4 \mid y \). We have \( x^{2p} = z^p - y^{2p} \), or
\[
(x^p)^2 = \frac{z^p - (y^2)^p}{z - y^2} (z - y^2).
\]

From \( 2p \mid y \) it follows that \( p \mid z - y^2 \), hence
\[
\left( \frac{z^p - (y^2)^p}{z - y^2}, z - y^2 \right) = 1.
\]

Thus
\[
\frac{z^p - (y^2)^p}{z - y^2} = e^2,
\]
where \( e \) is an odd positive integer; hence \( z^p - 1 + z^{p-2}y^2 + z^{p-3}(y^2)^2 \equiv 1 \pmod{8} \), \( 1 + z^{p-2}y^2 + z^{p-3}(y^2)^2 \equiv 1 \pmod{8} \), \( 1 + z^{p-2}y^2 \equiv 1 \pmod{8} \), \( y^2 \equiv 0 \pmod{8} \) and finally \( y \equiv 0 \pmod{4} \). Thus we have \( 4y^p \mid y \).

From \( (x^p + iy^p)(x^p - iy^p) = z^p \) we obtain
\[
x^p + iy^p = i^r (a + bi)^p, \quad r = 0, 1, 2, 3.
\]
The factor \( i^r \) can be absorbed into the \( p \)th power, and so we need only consider \( r = 0 \).

From \( (x, y) = 1 \) it follows that \( (a, b) = 1 \). Thus
\[
x^p + iy^p = (a + bi)^p, \quad (a, b) = 1,
\]
hence
\[
x^p = a^p + \left( \frac{p}{2} \right) a^{p-2} (bi)^2 + \left( \frac{p}{4} \right) a^{p-4} (bi)^4 + \ldots + \left( \frac{p}{p - 1} \right) a (bi)^{p-1},
\]
(7)
\[
iy^p = \left( \frac{p}{1} \right) a^{p-1} (bi) + \left( \frac{p}{3} \right) a^{p-3} (bi)^3 + \ldots + \left( \frac{p}{p - 2} \right) a^2 (bi)^{p-2} + (bi)^p.
\]

Since \( x^{2p} + y^{2p} = (a^2 + b^2)^p \), \( 2 \mid y \), \( 2 \mid x \), we have \( 2 \mid ab \). From \( 2 \nmid x \) and (7) it follows that \( 2 \nmid a \). Thus \( 2 \mid b \). Since \( p^2 \mid y \), (8) gives \( p \mid b \). Thus \( 2p \mid b \) and since \( (a, b) = 1 \) we have \( (a, 2p) = 1 \). From (7) we obtain
\[
x^p = a \left( a^{p-1} - \left( \frac{p}{2} \right) a^{p-2} b^2 + \left( \frac{p}{4} \right) a^{p-4} b^4 + \ldots + \left( \frac{p}{p - 1} \right) b^{p-1} \right).
\]
From \( (a, bp) = 1 \) it follows that
\[
\left( a, a^{p-1} - \left( \frac{p}{2} \right) a^{p-2} b^2 + \ldots + \left( \frac{p}{p - 1} \right) b^{p-1} \right) = 1.
\]
Thus
\[ a = a^p. \]
From (8) we get
\[
y^p = bp \left( a^{p-1} - \frac{1}{p} \binom{p}{3} a^{p-3} b^2 + \cdots \pm \frac{1}{p} \binom{p}{p-2} a^2 b^{p-3} \mp b^{p-1} \right),
\]
and since \((bp, a) = 1\) we have
\[
bp, a^{p-1} - \frac{1}{p} \binom{p}{3} a^{p-3} b^2 + \cdots \pm \frac{1}{p} \binom{p}{p-2} a^2 b^{p-3} \mp b^{p-1} = 1.
\]
From (11) it now follows that there exists a positive integer \(\beta\) such that
\[
bp, a^{p-1} - \frac{1}{p} \binom{p}{3} a^{p-3} b^2 + \cdots \pm \frac{1}{p} \binom{p}{p-2} a^2 b^{p-3} \mp b^{p-1} = \beta \frac{bp}{p},
\]
and since \((bp, a) = 1\) we have
\[
\beta = \frac{bp}{p} \quad \text{where} \ 4p^2 | \beta.
\]
From (6), (10) and (13) we get
\[
x^p + iy^p = \left( \alpha + \beta i \right) ^p, \quad \text{(14)}
\]
\[
x^p - iy^p = \left( \alpha - \beta i \right) ^p, \quad \text{(15)}
\]
and since \(z = \alpha^2 p + \beta^2 \frac{p}{p^2}\), and thus
\[
z = \alpha^2 p + \beta^2 \frac{p}{p^2}, \quad \text{(16)}
\]
From (14) and (15) we get
\[
x^p = \frac{1}{2} \left( \alpha^p + \beta i \frac{p}{p} \right) ^p + \frac{1}{2} \left( \alpha^p - \beta i \frac{p}{p} \right) ^p
\]
\[
= (\alpha^p)^p - \binom{p}{2} (\alpha^p)^{p-2} \left( \frac{\beta}{p} \right) ^2 + \binom{p}{4} (\alpha^p)^{p-4} \left( \frac{\beta}{p} \right) ^4 - \ldots,
\]
\[
y^p = \frac{1}{2i} \left[ (\alpha^p)^p - (\alpha^p - \beta i \frac{p}{p}) ^p \right]
\]
\[
= \frac{p}{1} (\alpha^p)^{p-1} \left( \frac{\beta}{p} \right) ^{p-1} \left( \frac{\beta}{p} \right) ^3 + \frac{p}{5} (\alpha^p)^{p-5} \left( \frac{\beta}{p} \right) ^5 + \ldots
\]
and formulas (3) and (4) are proved.
By the theorem of Vandiver we have \(z^p \equiv z \pmod{p^3}\), and since \((z, p) = 1\) we have \(z^{p-1} \equiv 1 \pmod{p^3}\). Since \(z = \alpha^2 p + \beta^2 \frac{p}{p^2}\) and \(4p^2 | \beta\) we have \(z^{p-1} \equiv (\alpha^2 p)^p \equiv 1 \pmod{p^3}\), and so
\[
\alpha^{p-1} \equiv 1 \pmod{p^3}.
\]
This completes the proof of Theorem 1.

Let \( z^p + y^p = z^p \) with \( (x, y, z) = 1, 0 < x < y \) and \( p > 2 \). Inkeri (in 1953) [4] showed that if \( p \nmid xyz \) then \( x > \left( \frac{(2p^3 + p)/\log 3p}{p} \right)^p \) and if \( p | xyz \) then \( x > x^p - 1 \)/\( 2p^p - 1 \). The author (in 1960) [8] proved that for any natural number \( n > 2, x^n + y^n = z^n \) implies \( x > 3n \), \( y > 3n \).

Inkeri and van der Poorten (in 1980) [5] proved that if \( x^p + y^p = z^p \) with \( (x, y, z) = 1, 0 < x < y \) and \( p > 2 \) then \( z^p - x > p^p p^2 \).

Brindza, Györy and Tijdeman (in 1985) [1] proved that for any natural number \( n > 2, x^n + y^n = z^n \) implies \( x > n^{n/3} \).

Here we shall prove the following

**Theorem 2.** If \( x^p + y^p = z^p \) with \( (x, y, z) = 1, 0 < x < y \) and \( p > 2 \) then \( z > p^{4p} \). If \( x^p + y^p = z^p \), \( (x, y, z) = 1, 0 < x < y \) and \( p > 2 \) then there exist coprime positive integers \( \alpha \) and \( \beta \) such that \( z^2 = \alpha^{2p} + \beta^{2p}/p^2 \), where \( 8p^3 | \beta, \alpha^p - 1 \equiv 1 \) (mod \( p^2 \)) and \( z > p^{3p} \).

**Proof.** Let \( x^p + y^p = z^p \). By (2) we have

\[
\begin{align*}
z = \alpha^2 p + \beta^{2p}/p^2 & > \left( \frac{4p^2}{p^2} \right)^p > p^{4p}.
\end{align*}
\]

Let \( x^p + y^p = z^p, 2 \mid y \). By Theorem of [9] we have \( 8p^3 \mid y \). From (11) and (12) it follows that \( \beta = bp \) and from \( 8p^3 \mid y \) and (12) we get \( (8p^3)^p | bp = \beta^p \), hence \( 8p^3 | \beta \) and \( z^2 = \alpha^{2p} + \beta^p/p^2, \alpha^p - 1 \equiv 1 \) (mod \( p^2 \)).

Thus

\[
\begin{align*}
z^2 & > \left( \frac{8p^3}{p^2} \right)^2 = \frac{8p^6}{p^2} > p^{6p},
\end{align*}
\]

hence \( z > p^{3p} \). This completes the proof of Theorem 2.

**REFERENCES**


