COLLOQUIUM MATHEMATICUM

VOL. LIII 1987 FASC. 1

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

BY

A. ROTKIEWICZ AND A. SCHINZEL (WARSZAWA)

It was shown by Chao Ko [1], [2] that the equation $x^p+1=z^2$ has no solutions in positive integers if p is a prime greater than 3. E. Z. Chein [3] and the first-named author [5] gave simpler proofs of Ko's result, G. Terjanian [8] proved that if x, y, z are positive integers such that $x^{2p}+y^{2p}=z^2$ then $2p$ divides x or y. In this paper we shall use some ideas contained in the quoted papers of Chein and Terjanian to prove the following extensions of Ko's and Terjanian's results.

THEOREM 1. *If $x^p+y^{2p}=z^2$, where p is a prime greater than 3, x, y and z are non-zero integers then*

$$p<2|y|, \quad |x|<8y^{2p+2}.$$

If $(x, y)=1$, $2|x$, $y>0$, $z>0$ then $8|x$ and there exists another solution satisfying the same conditions.

THEOREM 2. *If x, y, z are positive integers such that $x^{2p}+y^{2p}=z^2$ then $4p|x$ or $4p|y$.*

Remark 1. According to a result of Shorey [8] if $(x, z)=1$ and $|x|>1$ the greatest prime factor of z^2-x^p is greater than $c\left(\frac{\log p}{\log\log p}\right)^{1/2}$, where c is a positive constant. It follows that under the assumptions of Theorem 1 both x and y have a prime factor greater than $c\left(\frac{\log p}{\log\log p}\right)^{1/2}$.

The proofs of our theorems are based on three lemmas.

LEMMA 1. *Let $(x, y)=1$ and p be a prime >3. If $p|z$, $2\nmid z$ or $p\nmid z$, $2|z$ then the equation $x^p+y^p=z^2$ is impossible.*

For the proof see [6].

LEMMA 2. *If p is an odd prime and $(x, y)=1$, $p\nmid x+y$ then*

$$\left(\frac{x^p+y^p}{x+y}, x+y\right)=1.$$

This lemma is notorious and its proof may be omitted.

LEMMA 3. *If under the assumptions of Theorem* 1, $(x, y) = 1$, $2|x$ *and* $y > 0$ *then there exist coprime positive integers* a, b *and an* $\varepsilon = \pm 1$ *such that* $a > b$, $2|ab$

$$y|ab, \quad \left(\frac{ab}{y}, y\right) = 1 \tag{1}$$

and either

$$4^{p-1}\left(\frac{ab}{y}\right)^p = (a-\varepsilon b)^p + \varepsilon y^p, \quad x = \frac{4ab(a-\varepsilon b)}{y} \tag{2}$$

or

$$4^{p-1}\left(\frac{ab}{y}\right)^p = y^p - (a-b)^p, \quad x = \frac{-4ab(a-b)}{y}. \tag{3}$$

Proof. From $(x, y) = 1$, $x^p + y^{2p} = z^2$ it follows that $(y, z) = 1$ and from $2|x$ we obtain $(z + y^p, z - y^p) = 2$. Thus $x^p = (z - y^p)(z + y^p)$ and for a suitable $\varepsilon = \pm 1$

$$z + \varepsilon y^p = 2^{p-1} x_1^p,$$

$$z - \varepsilon y^p = 2x_2^p,$$

$$x = 2x_1 x_2, \quad 2 \nmid x_2, \quad (x_1, x_2) = 1.$$

Consequently, $2\varepsilon y^p = 2^{p-1} x_1^p - 2x_2^p$; hence

$$x_2^p = 2^{p-2} x_1^p - \varepsilon y^p. \tag{4}$$

But (4) holds if and only if

$$(2\varepsilon x_1 y)^p + (x_2^2)^p = (x_2^p + 2\varepsilon y^p)^2. \tag{5}$$

From $2 \nmid x_2$ it follows that $2 \nmid x_2^p + 2\varepsilon y^p$. Since $(x_1, x_2) = 1$, $2 \nmid x_2$, $(x, y) = 1$, $x_2 | x$, we have $(2\varepsilon x_1 y, x_2^2) = 1$. If $p | x_2^p + 2\varepsilon y^p$ then by Lemma 1 the equation (5) is impossible. Thus we can assume that $p \nmid x_2^p + 2\varepsilon y^p$. By Lemma 2 we have

$$\left(\frac{(2\varepsilon x_1 y)^p + (x_2^2)^p}{2\varepsilon x_1 y + x_2^2}, 2\varepsilon x_1 y + x_2^2\right) = 1$$

and (5) implies

$$2\varepsilon x_1 y + x_2^2 = h^2, \quad \text{where } h | x_2^p + 2\varepsilon y^p, \ h > 0. \tag{6}$$

But (6) holds if and only if

$$(hx_2)^2 + (x_1 y)^2 = (x_2^2 + \varepsilon x_1 y)^2. \tag{7}$$

The equalities $(x_1, x_2) = 1$, $(y, x_2) = 1$, $h^2 = 2\varepsilon x_1 y + x_2^2$ imply $(hx_2, x_1 y) = 1$. Since x_2 is odd, so is h; thus $4 | h^2 - x_2^2$ and $2 | x_1 y$. Hence the solutions of (7) are given by

$$h|x_2| = a^2 - b^2, \quad |x_1| y = 2ab, \quad |x_2^2 + \varepsilon x_1 y| = a^2 + b^2,$$

where a, b are coprime positive integers, $a > b$, $2 | ab$. The equality $x_2^2 + \varepsilon x_1 y = -(a^2 + b^2)$ would imply

$$x_2^2 = x_2^2 + \varepsilon x_1 y - \varepsilon x_1 y = -(a + \varepsilon b \operatorname{sgn} x_1)^2,$$

which is impossible. Thus $x_2^2 + \varepsilon x_1 y = a^2 + b^2$ and

$$x_2^2 = x_2^2 + \varepsilon x_1 y - \varepsilon x_1 y = (a - \varepsilon b \operatorname{sgn} x_1)^2$$

and since $a > b$,

$$|x_2| = a - \varepsilon b \operatorname{sgn} x_1, \quad |x_1| = \frac{2ab}{y}. \tag{8}$$

Since $(x_1, y) = 1$, we get (1). If $x > 0$ there is no loss of generality in assuming $x_1 > 0$, $x_2 > 0$ and then (4) and (8) give (2). If $x < 0$ (4) gives

$$-|x_2|^p = 2^{p-2} |x_1|^p - \varepsilon y^p \operatorname{sgn} x_1;$$

thus $\varepsilon \operatorname{sgn} x_1 = 1$ and (8) implies (3).

Proof of Theorem 1. Let $x^p + y^{2p} = z^2$, where p is a prime > 3 and x, y, z are non-zero integers. We assume without loss of generality that $y > 0$, $z > 0$. We shall consider successively the following cases:

(i) $(x, y) = 1$, $2 | x$, $x > 0$;
(ii) $(x, y) = 1$, $2 | x$, $x < 0$;
(iii) $(x, y) = 1$, $2 \nmid x$;
(iv) $(x, y) \neq 1$.

In the case (i) by Lemma 3 there exist coprime positive integers a, b and an $\varepsilon = \pm 1$ such that $a > b$, $2 | ab$ and (1), (2) hold. We must have $b < y$, otherwise the left-hand side of (2) is greater than the right-hand side.

Assume first that $a < 6y^2$. Since x is even, y is odd,

$$\frac{(a - \varepsilon b)^p + \varepsilon y^p}{a - \varepsilon b + \varepsilon y} \equiv 1 \pmod 2$$

and (2) gives

$$4^{p-1} | a - \varepsilon b + \varepsilon y \quad \text{and} \quad 4^{p-1} \leqslant a + y < 6y^2 + y.$$

Hence $p < 2y + 1$ and since p is odd, $p < 2y$. Moreover, (2) gives

$$\frac{a}{(a, y)} | \varepsilon (y^p - b^p);$$

hence

$$a \leqslant (a, y)(y^p - b^p) < y^{p+1}$$

and by (2)

$$x = \frac{4ab(a-\varepsilon b)}{y} < 8a^2 < 8y^{2p+2}. \tag{9}$$

Assume now that $a \geqslant 6y^2$. Since y is odd, we have $y \neq 4b$. If we had $y \geqslant 4b + 1$ it would follow

$$\left(\frac{4ab}{y}\right)^p \leqslant a^p \left(\frac{y-1}{y}\right)^p.$$

On the other hand,

$$(a-\varepsilon b)^p + \varepsilon y^p > \begin{cases} a^p\left(1-\frac{b}{a}\right)^p \geqslant a^p\left(1-\frac{1}{6y}\right)^p & \text{if } \varepsilon = 1, \\ a^p\left(1-\left(\frac{y}{a}\right)^p\right) \geqslant a^p\left(1-\frac{1}{6y}\right)^p & \text{if } \varepsilon = -1. \end{cases}$$

Thus we would get from (2)

$$\left(\frac{y-1}{y}\right)^p > 4\left(1-\frac{1}{6y}\right)^p,$$

a contradiction. Therefore, $y \leqslant 4b-1$ thus

$$\left(\frac{4ab}{y}\right)^p \geqslant a^p \left(\frac{y+1}{y}\right)^p.$$

On the other hand,

$$(a-\varepsilon b)^p + \varepsilon y^p < \begin{cases} a^p\left(1+\left(\frac{y}{a}\right)^p\right) < a^p\left(1+\frac{1}{6y}\right)^p & \text{if } \varepsilon = 1, \\ a^p\left(1+\frac{b}{a}\right)^p < a^p\left(1+\frac{1}{6y}\right)^p & \text{if } \varepsilon = -1. \end{cases}$$

Therefore, we get from (2)

$$\left(\frac{y+1}{y}\right)^p < 4\left(1+\frac{1}{6y}\right)^p,$$

$$\left(1+\frac{5}{6y+1}\right)^p < 4.$$

Since $y > b \geqslant 1$, we have $y \geqslant 3$ and

$$\left(1+\frac{5}{6y+1}\right)^{2y} \geqslant \left(\frac{24}{19}\right)^6 > 4.$$

Thus $p < 2y$ and the estimate (9) for x is proved as before.

In the case (ii) by Lemma 3 there exist coprime positive integers a, b such that $a > b$, $2|ab$ and (1), (3) hold. Since.

$$\frac{y^p-(a-b)^p}{y-(a-b)} \equiv 1 \pmod 2,$$

it follows from (3) that

$$4^{p-1} | y-(a-b), \quad 4^{p-1} \leqslant y-(a-b) < y$$

and trivially $p < 2y$.

The equation $x^p+y^{2p} = z^2$ gives directly $|x| < y^2 < 8y^{2p+2}$.

In the case (iii) $x^p+y^{2p} = z^2$ implies

$$x^p = (z-y^p)(z+y^p), \quad (z-y^p, z+y^p) = 1$$

and

$$z-y^p = x_1^p, \quad z+y^p = x_2^p, \; x_2 > |x_1|,$$

$$x_2^p - x_1^p = 2y^p. \tag{10}$$

In virtue of Zsigmondy's theorem [10] the left-hand side has a prime factor of the form $pk+1$. Since it divides y, we have $y \geqslant 2p+1$.

If $x_2 < p$ we have $|x| = |x_1| x_2 < x_2^2 < p^2 < y^2$.

If $x_2 \geqslant p$ we have

$$x_2^p - x_1^p \geqslant x_2^p - (x_2-2)^p > 2x_2^{p-1},$$

and (10) gives

$$2x_2^{p-1} < 2y^p; \quad x_2 < y^{p/(p-1)}.$$

Hence $|x| = |x_1| x_2 < x_2^2 < y^{2p/(p-1)} < y^3$.

In the case (iv) we proceed by induction with respect to (x, y). If $(x, y) = 1$ the theorem holds as we have just proved. Assume that it holds if $(x, y) < d$ and let $(x, y) = d > 1$. If q is a prime dividing d and

$$q^\alpha \| x, \; q^\beta \| y, \; q^\gamma \| z$$

we infer from $x^p+y^{2p} = z^2$ that either $2\beta \leqslant \alpha$, $p\beta \leqslant \gamma$ or $2\beta > \alpha$ and $p\alpha = 2\gamma$, in which case α is even. Let us put

$$\delta = \begin{cases} \beta & \text{if } 2\beta \leqslant \alpha, \\ \alpha/2 & \text{if } 2\beta > \alpha. \end{cases}$$

The numbers $xq^{-2\delta}$, $yq^{-\delta}$ and $zq^{-p\delta}$ satisfy the same equation as x, y, z, moreover $(xq^{-2\delta}, yq^{-\delta}) \leqslant dq^{-\delta} < d$. Hence by the inductive assumption

$$p < 2yq^{-\delta}, \quad |xq^{-2\delta}| < 8(yq^{-\delta})^{2p+2}$$

and $p < 2y$, $|x| < 8y^{2p+2}$. The inductive proof of the first part of the theorem is complete.

To prove the second part let us note that if $(x, y) = 1$, $2|x$, $y > 0$, $z > 0$ then by Lemma 3

$$\text{either } x > 0,\ xy = 4ab(a-\varepsilon b) \text{ or } x < 0,\ xy = -4ab(a-b)$$

and $2|ab$, $2 \nmid y$ implies $x \equiv 0 \pmod 8$. Moreover by (5) the equation $x^p + y^{2p} = z^2$ besides the solution $\langle 2x_1 x_2, y, 2x_2^p + \varepsilon y^p\rangle$ has also the solution $\langle 2\varepsilon x_1 y, |x_2|, |x_2^p + 2\varepsilon y^p|\rangle$. If the two solutions in question were identical we should have $x_2 = \varepsilon y$, $y = 1$, $2\varepsilon + \varepsilon = 3$, $(2\varepsilon x_1)^p + 1 = 3^2$, which is impossible for $p > 3$.

This completes the proof of Theorem 1.

Remark 2. By using estimates for linear form in logarithms of algebraic numbers one can drastically improve the bound for p in the case of x even, $(x, y) = 1$. Unfortunately we cannot do it in the case of x odd.

Proof of Theorem 2. If $x^{2p} + y^{2p} = z^2$, $(x, y) = 1$, $2|x$ we infer from Lemma 3 that for some coprime positive integers a, b and an $\varepsilon = \pm 1$

$$x^2 = \frac{4ab(a-\varepsilon b)}{|y|}, \quad 4^{p-1}\left(\frac{ab}{y}\right)^p = (a-\varepsilon b)^p + \varepsilon y^p.$$

Hence $\dfrac{ab}{|y|} = c^2$, $(2^{p-1}c^p)^2 = (a-\varepsilon b)^p + \varepsilon y^p$. By Lemma 1 we have $p|c$; hence $p|x$ and since $8|x^2$, it follows that $4p|x$.

If $2 \nmid x$ then $2|y$ and by symmetry $4p|y$.

Remark 3. According to a theorem of Vandiver (see [4], Satz 1046) if $x^p + y^p + z^p = 0$, where $(x, y, z) = 1$ and p is an odd prime then

$$x^p \equiv x \pmod{p^3}, \quad y^p \equiv y \pmod{p^3}, \quad z^p \equiv z \pmod{p^3}.$$

Combining this result with Theorem 2, we get that if $x^{2p} + y^{2p} = z^{2p}$ then $4p^2|x$ or $4p^2|y$ (by a more delicate argument given in [7] even $8p^3|x$ or $8p^3|y$). Unfortunately we have no similar result for the equation $x^{2p} + y^{2p} = z^2$.

Note added in proof. It follows from the Faltings theorem [11] that the equation $x^p + y^{2p} = z^2$ has only finitely many solutions satisfying $(x, y) = 1$ for every given prime $p > 3$.

REFERENCES

[1] Chao Ko, Acta Scientiarum Naturalium Universitatis Szechuanensis 2 (1960), p. 57–64.
[2] – *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$, Scientia Sinica 14 (1965), p. 457–460.
[3] E. Z. Chein, *A note on the equation* $x^2 = y^q + 1$, Proceedings of the American Mathematical Society 56 (1976), p. 83–84.
[4] E. Landau, *Vorlesungen über Zahlentheorie*, Bd. III, *Aus der algebraischen Zahlentheorie. Über das Fermatsche Vermutung*, Leipzig 1927, reprint Chelsea 1974.
[5] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arithmetica 42 (1983), p. 163–187.
[6] – *On the equation* $x^p + y^p = z^2$, Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques 30 (1982), p. 211–214.
[7] – *On Fermat's equation with exponent* $2p$, Colloquium Mathematicum 45 (1981), p. 101–102.
[8] T. N. Shorey, *On the greatest prime factor of* $(ax^m + by^n)$, Acta Arithmetica 36 (1980), p. 21–25.
[9] G. Terjanian, *L'équation* $x^p - y^p = az^2$ *et le théorème de Fermat*, Séminaire de théorie des nombres de Bordeaux, Année 1977–1978, exposé n° 29.
[10] A. Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte für Mathematik und Physik 3 (1882), p. 265–284.
[11] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Mathematicae 73 (1983), p. 349–366; *Erratum*, ibidem 75 (1984), p. 381.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA, POLAND

Reçu par la Rédaction le 20. 07. 1982