COLLOQUIUM MATHEMATICUM

VOL. LXII 1991 FASC. I

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 $8p^3 \mid x$ or $8p^3 \mid y$.

In [10] the impossibility of the diophantine equation $x^p + y^p = z^2$ was established under the conditions $(x, y) = 1$, and either $p \mid z$, $2 \nmid z$, or $p \nmid z$, $2 \mid z$ (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 $x^{2p} + y^{2p} = z^2$ where p is a prime greater than 3 then either $4p \mid x$ or $4p \mid y$, 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 $x^{2p} + y^{2p} = z^2$ then either $2p \mid x$ or $2p \mid y$, 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*

$$x^{2p} + y^{2p} = z^p \tag{1}$$

then either $4p^2 \mid x$ or $4p^2 \mid y$, and there exist coprime positive integers α and β such that

$$z = \alpha^{2p} + \frac{\beta^{2p}}{p^2} \qquad \textit{where } 4p^2 \mid \beta \textit{ and } \alpha^{p-1} \equiv 1 \pmod{p^2}, \tag{2}$$

$$x^p = (\alpha^p)^p - \binom{p}{2}(\alpha^p)^{p-2}\left(\frac{\beta^p}{p}\right)^2 + \binom{p}{4}(\alpha^p)^{p-4}\left(\frac{\beta^p}{p}\right)^4 - \ldots, \tag{3}$$

$$y^p = \binom{p}{1}(\alpha^p)^{p-1}\left(\frac{\beta^p}{p}\right) - \binom{p}{3}(\alpha^p)^{p-3}\left(\frac{\beta^p}{p}\right)^3 + \binom{p}{5}(\alpha^p)^{p-5}\left(\frac{\beta^p}{p}\right)^5 - \ldots \tag{4}$$

P r o o f. 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 $(y^p)^2=z^p+(-x^2)^p$ 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 $p\mid y$, $p\ge 3$, 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

$$(x^p)^2=\frac{z^p-(y^2)^p}{z-y^2}(z-y^2)\,. \tag{5}$$

From $2p\mid y$ it follows that $p\nmid z-y^2$, 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 $4p^2\mid y$.

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 pth power, and so we need only consider $r=0$.

From $(x,y)=1$ it follows that $(a,b)=1$. Thus

$$x^p+iy^p=(a+bi)^p,\quad (a,b)=1\,, \tag{6}$$

hence

$$x^p=a^p+\binom{p}{2}a^{p-2}(bi)^2+\binom{p}{4}a^{p-4}(bi)^4+\ldots+\binom{p}{p-1}a(bi)^{p-1}, \tag{7}$$

$$iy^p=\binom{p}{1}a^{p-1}(bi)+\binom{p}{3}a^{p-3}(bi)^3+\ldots+\binom{p}{p-2}a^2(bi)^{p-2}+(bi)^p\,. \tag{8}$$

Since $x^{2p}+y^{2p}=(a^2+b^2)^p$, $2\mid y$, $2\nmid x$, 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

$$x^p=a\left(a^{p-1}-\binom{p}{2}a^{p-3}b^2+\binom{p}{4}a^{p-5}b^4+\ldots\pm\binom{p}{p-1}b^{p-1}\right)\,. \tag{9}$$

From (a,bp)=1 it follows that

$$\left(a, a^{p-1}-\binom{p}{2}a^{p-2}b^2+\ldots\pm\binom{p}{p-1}b^{p-1}\right)=1\,.$$

Thus

$$a = \alpha^p\,. \tag{10}$$

From (8) we get

$$y^p = bp\left(a^{p-1} - \frac{1}{p}\binom{p}{3}a^{p-3}b^2 + \ldots \pm \frac{1}{p}\binom{p}{p-2}a^2b^{p-3} \mp \frac{b^{p-1}}{p}\right), \tag{11}$$

and since $(bp, a) = 1$ we have

$$\left(bp, a^{p-1} - \frac{1}{p}\binom{p}{3}a^{p-3}b^2 + \ldots \pm \frac{1}{p}\binom{p}{p-2}a^2b^{p-3} \mp \frac{b^{p-1}}{p}\right) = 1\,. \tag{12}$$

From (11) it now follows that there exists a positive integer β such that $\beta^p = bp$. Since $4p^2 \mid y$, (11) and (12) show that $(4p^2)^p \mid bp = \beta^p$, hence $4p^2 \mid \beta$. Thus

$$b = \beta^p/p \quad \text{where } 4p^2 \mid \beta\,. \tag{13}$$

From (6), (10) and (13) we get

$$x^p + iy^p = \left(\alpha^p + \frac{\beta^p}{p}i\right)^p, \tag{14}$$

$$x^p - iy^p = \left(\alpha^p - \frac{\beta^p}{p}i\right)^p, \tag{15}$$

hence $z^p = (\alpha^{2p} + \beta^{2p}/p^2)^p$, and thus

$$z = \alpha^{2p} + \frac{\beta^{2p}}{p^2}\,. \tag{16}$$

From (14) and (15) we get

$$\begin{aligned}
x^p &= \frac{1}{2}\left(\alpha^p + \frac{\beta^p}{p}i\right)^p + \frac{1}{2}\left(\alpha^p - \frac{\beta^p}{p}i\right)^p \\
&= (\alpha^p)^p - \binom{p}{2}(\alpha^p)^{p-2}\left(\frac{\beta^p}{p}\right)^2 + \binom{p}{4}(\alpha^p)^{p-4}\left(\frac{\beta^p}{p}\right)^4 - \ldots, \\
y^p &= \frac{\left(\alpha^p + \frac{\beta^p}{p}i\right)^p - \left(\alpha^p - \frac{\beta^p}{p}i\right)^p}{2i} \\
&= \binom{p}{1}(\alpha^p)^{p-1}\left(\frac{\beta^p}{p}\right) - \binom{p}{3}(\alpha^p)^{p-3}\left(\frac{\beta^p}{p}\right)^3 + \binom{p}{5}(\alpha^p)^{p-5}\left(\frac{\beta^p}{p}\right)^5 + \ldots
\end{aligned}$$

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 $z = \alpha^{2p} + \beta^{2p}/p^2$ and $4p^2 \mid \beta$ we have $z^{p-1} \equiv (\alpha^{2p})^{p-1} \pmod{p^3}$, and so

$$\alpha^{p-1} \equiv 1 \pmod{p^2}\,. \tag{17}$$

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 $x > ((2p^3 + p)/log3p)^p$, and if $p \mid xyz$ then $x > p^{3p-4}$ and $y > \frac{1}{2}p^{3p-1}$. The author (in 1960) [8] proved that for any natural number $n > 2$, $x^n + y^n = z^n$ implies $x > 3^n$, $y > 3^n$.

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 $z - x > 2^p p^{2p}$.

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

Here we shall prove the following

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

Proof. Let $x^{2p} + y^{2p} = z^p$. By (2) we have

$$z = \alpha^{2p} + \frac{\beta^{2p}}{p^2} > \frac{(4p^2)^{2p}}{p^2} > p^{4p} .$$

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

Thus

$$z^2 > \frac{(8p^3)^{2p}}{p^2} = \frac{8^{2p} p^{6p}}{p^2} > p^{6p} ,$$

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

REFERENCES

[1] B. Brindza, K. Győry and R. Tijdeman, *The Fermat equation with polynomial values as base variables*, Invent. Math. 80 (1985), 139–151.

[2] Chao Ko, Acta Sci. Natur. Univ. Szechuanensis 2 (1960), 57–64.

[3] —, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$*, Sci. Sinica Ser. A 14 (1965), 457–460.

[4] K. Inkeri, *Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem*, Ann. Univ. Turku. Ser. A I 16 (1953), 9 pp.

[5] K. Inkeri and A. J. van der Poorten, *Some remarks on Fermat's conjecture*, Acta Arith. 36 (1980), 107–111.

[6] E. Landau, *Vorlesungen über Zahlentheorie*, Bd. III, Leipzig 1927; reprint Chelsea, 1974.

[7] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, New York 1979.

[8] A. Rotkiewicz, *Une remarque sur le dernier théorème de Fermat*, Mathesis 69 (1960), 135–140.

[9] —, *On Fermat's equation with exponent 2p*, Colloq. Math. 45 (1981), 101–102.

[10] A. Rotkiewicz, *On the equation $x^p + y^p = z^2$*, Bull. Acad. Polon. Sci. Sér. Sci. Math. 30 (1982), 211–214.
[11] A. Rotkiewicz and A. Schinzel, *On the diophantine equation $x^p + y^{2p} = z^p$*, Colloq. Math. 53 (1987), 147–153.
[12] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, 1981.
[13] G. Terjanian, *Sur l'équation $x^{2p} + y^{2p} = z^{2p}$*, C. R. Acad. Sci. Paris Sér. A–B 285 (1977), 973–975.
[14] —, *L'équation $x^p - y^{2p} = az^2$ et le théorème de Fermat*, Séminaire de théorie des nombres de Bordeaux, Année 1977–1978, exposé no. 29.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
ŚNIADECKICH 8
00-950 WARSZAWA, POLAND

Reçu par la Rédaction le 15.1.1990