COLLOQUIUM MATHEMATICUM

VOL. LIV 1987 FASC. 1

A NOTE ON THE FERMAT EQUATION

BY

R. TIJDEMAN (LEIDEN)

We consider the Fermat equation with even exponents,

$$x^{2n}+y^{2n} = z^{2n} \quad \text{in integers } n > 1,\ x > 0,\ y > 0,\ z > 0. \tag{1}$$

Without loss of generality we may assume $x < y < z$. Fermat proved that (1) has no solutions with n even (see [3]). Terjanian [6] showed that (1) has no solutions with n prime and $n \nmid xyz$. Wagstaff [7] proved that there are no solutions with $n < 125000$. It follows from Faltings' celebrated solution of the Mordell conjecture [1] that for every n equation (1) has only finitely many primitive solutions. Stewart [5] and Inkeri and van der Poorten [2], independently, showed by Baker's method on linear forms in logarithms that there are only finitely many solutions of (1) for which $y-x$ is bounded. Stewart gave a lower bound for $y-x$ in terms of n and z. It follows from an old lemma of Barlow and Abel that (1) has only a finite number of solutions if $z-y$ is bounded, but larger than 2. We shall prove by elementary estimations that (1) has no solutions at all with $z-y = 1$ or 2.

THEOREM. *If* (1) *holds, then* $z-y \geqslant 2^{2n-1}/n$.

Note that Wagstaff's bound now implies that

$$z-y \geqslant 2^{249999}/125000 \geqslant 10^{75000}.$$

The proof of the Theorem depends on the following lemma of Barlow and Abel.

LEMMA 1. *Suppose m, x, y, z are positive integers with $x < y < z$ and $(x, y, z) = 1$ such that*

$$x^m + y^m = z^m.$$

Then

(a) *there exist $\delta \in \{0, 1\}$ and positive integers a_1, d_1 with $d_1|m$ such that*

$$z-y = 2^{\delta} d_1^{-1} a_1^m.$$

(b) *Suppose m is odd. Then there exist positive integers a_2, d_2 with $d_2|m$*

such that

$$x+y = d_2^{-1} a_2^m.$$

The proof is well known (see [4], Chapter 11).

The next lemma shows that y is large compared to n.

LEMMA 2. *If* (1) *holds, then* $y^2 \geqslant 2^n/(2n)$ *and* $y \geqslant 10n^2$.

Proof. By Fermat's result, n is odd. By Lemma 1 (b), there exists integers a and d with $d|n$ such that $x^2+y^2 = d^{-1}a^n$. Hence $a > 1$ and $y^2 > a^n/(2n) \geqslant 2^n/(2n)$. By Wagstaff's result, we have $n > 100$. (Of course, much older results suffice.) Thus

$$y \geqslant (2^n/(2n))^{1/2} \geqslant 10n^2.$$

Proof of the Theorem. Suppose that (1) holds. Without loss of generality we may assume $(x, y) = 1$, $x < y < z$ and n odd. We distinguish between three cases.

Case 1. Assume $z-y = 1$. Then z odd, y even, x odd. By writing $(x^n)^2+(y^n)^2 = (z^n)^2$ we see that there exist positive integers r, s with $r > s > 0$, $(r, s) = 1$, and rs even such that

$$x^n = r^2-s^2, \quad y^n = 2rs, \quad z^n = r^2+s^2. \tag{2}$$

Since $r^2+s^2 = z^n = (y+1)^n$, by Lemma 2 we have

$$\begin{aligned} y^n+ny^{n-1} < r^2+s^2 &= y^n+\binom{n}{1}y^{n-1}+\binom{n}{2}y^{n-2}+\ldots \\ &< y^n+ny^{n-1}\left(1+\frac{n}{2y}+\left(\frac{n}{2y}\right)^2+\ldots\right) < y^n+2ny^{n-1}. \end{aligned} \tag{3}$$

Furthermore, by Lemma 2,

$$\begin{aligned} (r^2-s^2)^2 = x^{2n} = (y+1)^{2n}-y^{2n} &= \binom{2n}{1}y^{2n-1}+\binom{2n}{2}y^{2n-2}+\ldots \\ &< 2ny^{2n-1}\left(1+\frac{n}{y}+\frac{n^2}{y^2}+\ldots\right) < 3ny^{2n-1}. \end{aligned}$$

Hence

$$\sqrt{2n}\,y^{n-1/2} < r^2-s^2 < \sqrt{3n}\,y^{n-1/2}. \tag{4}$$

Combining (3) and (4), by Lemma 2 we obtain

$$y^n < 2r^2 < y^n+2\sqrt{n}\,y^{n-1/2}$$

and

$$y^n-2\sqrt{n}\,y^{n-1/2} < 2s^2 < y^n.$$

This implies

$$(5)\qquad \frac{1}{\sqrt{2}}y^{n/2} < r < \frac{1}{\sqrt{2}}y^{n/2}+\sqrt{n}\,y^{n/2-1/2},$$

and, by Lemma 2,

$$(6)\qquad \frac{1}{\sqrt{2}}y^{n/2}-\sqrt{n}\,y^{n/2-1/2} < s < \frac{1}{\sqrt{2}}y^{n/2}.$$

Observe that $(r+s, r-s) = 1$ and $(r+s)(r-s) = x^n$ imply that $r+s = x_1^n$ for some positive integer x_1. Furthermore, either r even, s odd or r odd, s even. In the first instance, $(2r, s) = 1$, $2rs = y^n$, whence $2r = y_3^n$ for some $y_3 \in \boldsymbol{Z}$; in the second one, $(r, 2s) = 1$, $2rs = y^n$, whence $2s = y_3^n$ for some $y_3 \in \boldsymbol{Z}$. We have, by (5) and (6),

$$(7)\qquad |x_1^n - y_3^n| \leqslant \max(|r+s-2r|, |r+s-2s|) = r-s < 2\sqrt{n}\,y^{n/2-1/2}.$$

On the other hand, by (6),

$$\min(x_1^n, y_3^n) \geqslant 2s > \sqrt{2}\,y^{n/2}-2\sqrt{n}\,y^{n/2-1/2}.$$

Hence, by Lemma 2,

$$\min(x_1^n, y_3^n) \geqslant y^{n/2}+\big((\sqrt{2}-1)\,y^{1/2}-2\sqrt{n}\big)\,y^{n/2-1/2} > y^{n/2}.$$

Thus $\min(x_1, y_3) > \sqrt{y}$. Since $x_1 \neq y_3$, this implies

$$|x_1^n - y_3^n| \geqslant (\sqrt{y}+1)^n-(\sqrt{y})^n > ny^{n/2-1/2}.$$

Since $n > 4$, this yields a contradiction to (7).

Case 2. Assume $z-y = 2$. Then x even and y odd. Hence there exist positive integers r, s with $r > s > 0$, $(r, s) = 1$, rs even such that

$$(8)\qquad x^n = 2rs, \quad y^n = r^2-s^2, \quad z^n = r^2+s^2.$$

Since $(r, s) = 1$ and r^2-s^2 is odd, there exist positive integers y_1, y_2 such that

$$(9)\qquad r-s = y_1^n, \quad r+s = y_2^n.$$

We have, by Lemma 2,

$$\begin{aligned} 2s^2 &= z^n-y^n = (y+2)^n-y^n \\ &= 2ny^{n-1}\left(1+\frac{n-1}{2}\frac{2}{y}+\frac{(n-1)(n-2)}{2\cdot 3}\frac{4}{y^2}+\ldots\right) \\ &\leqslant 2ny^{n-1}\left(1+\frac{n}{y}+\frac{n^2}{y^2}+\ldots\right) < 4ny^{n-1}. \end{aligned}$$

This implies $s \leqslant 2n^{1/2} y^{(n-1)/2}$. Further, by (9) and (8), $y_2 > r^{1/n} > y^{1/2}$. Hence, by (9),

$$y_2^n - y_1^n = 2s \leqslant 4n^{1/2} y^{(n-1)/2} \leqslant 4n^{1/2} y_2^{n-1}.$$

On the other hand, $y_2 > y_1$, and therefore, by Lemma 2,

$$y_2^n - y_1^n \geqslant y_2^n - (y_2 - 1)^n = ny_2^{n-1} - \binom{n}{2} y_2^{n-2} + \binom{n}{3} y_2^{n-3} + \ldots$$

$$\geqslant ny_2^{n-1} \left(1 - \frac{n}{2y_2} - \left(\frac{n}{2y_2}\right)^3 - \ldots\right) \geqslant \frac{1}{2} ny_2^{n-1}.$$

Combining these inequalities we obtain $\frac{1}{2}n \leqslant 4n^{1/2}$, which is impossible.

Case 3. Assume $z - y > 2$. According to Lemma 1 (a), there exist integers δ, a, d with $\delta \in \{0, 1\}$ and $d | 2n$ such that $z - y = 2^\delta d^{-1} a^{2n}$. Hence $a > 1$ and $z - y \geqslant 2^{2n}/(2n)$.

Remark 1. An improvement of the estimate in Theorem 1, at least for large n, is possible by using van der Poorten's p-adic analogue of Baker's method (see [2]).

Remark 2. The proof that

$$x^n + y^n = z^n \quad \text{in integers } n > 1,\ x > 0,\ y > 0,\ z > 0 \tag{10}$$

has no solutions with n prime and $z - y = 1$ would settle Abel's conjecture that (10) has no solutions such that one among x^n, y^n, z^n is a prime power (see [3], Chapter IV).

REFERENCES

[1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), pp. 349–366.

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

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

[4] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge 1986.

[5] C. L. Stewart, *A note on the Fermat equation*, Mathematika 24 (1977), pp. 130–132.

[6] G. Terjanian, *Sur l'équation $x^{2p} + y^{2p} = z^{2p}$*, C. R. Acad. Sci. Paris 285 (1977), pp. 973–975.

[7] S. S. Wagstaff, Jr., *The irregular primes to 125000*, Math. Comp. 32 (1978), pp. 583–591.

MATHEMATISCH INSTITUUT R.U.
2300 RA LEIDEN
THE NETHERLANDS

Reçu par la Rédaction le 23.2.1984