A NOTE ON THE EQUATION $x^2 = y^q + 1$

E. Z. CHEIN

Abstract. It is proved here that the equation $x^2 = y^q + 1$ has no solution in natural numbers $x$, $y$ for which $q$ is a prime $> 3$.

It was shown by Chao Ko [1], [2] that the equation $x^2 = y^q + 1$ has no solution in natural numbers $x$, $y$ where $q$ is a prime $> 3$.

It is the purpose of this note to give a simpler proof of Ko Chao's result.
Throughout this note all symbols denote natural numbers, and notation $(a, b) = g$ means $g$ is the greatest common divisor of $a$ and $b$.

Auxiliary lemmas. Lemmas 1 and 2 are collections of some well-known results. The third is due to Nagell [3].

Lemma 1. If $q$ is an odd prime and $(x, y) = 1$, then $x + y$ divides $x^q + y^q$ and $(x + y, (x^q + y^q)/(x + y)) = q$ or 1 according as $x + y$ is divisible by $q$ or not.

Lemma 2. All the primitive solutions of equation $x^2 + y^2 = z^2$ for which $y$ is an even number are given by the formulas

$$x = a^2 - b^2, \quad y = 2ab \quad \text{and} \quad z = a^2 + b^2 \quad (a > b).$$

Lemma 3. If $x^2 = y^q + 1$ with $q$ prime and $x \geq 1, y \geq 1$, then $2 \mid y$ and $q \mid x$.

Principal result.

Theorem. Let $q$ be a prime $> 3$. The equation $x^2 = y^q + 1$ has no solution in natural numbers.

Proof. Let us assume now that there exist $x$, $y$ and a prime $q$ for which $x^2 = y^q + 1$.

It follows from Lemma 3 that $q \mid x$ and $2 \mid y$. Since $2 \mid x$, by Lemma 3 we have $(x + 1, x - 1) = 2$. Thus either

(I) $x + 1 = 2^{q-1}y_1^q, \quad x - 1 = 2y_2^q, \quad \text{or}$

(II) $x + 1 = 2y_2^q, \quad x - 1 = 2^{q-1}y_1^q$

holds, where $y = 2y_1y_2$, $2 \mid y_2$ and $(y_1, y_2) = 1$.

Case I. Suppose $x + 1 = 2^{q-1}y_1^q$ and $x - 1 = 2y_2^q$. It follows from $y_2^q = 2^{q-2}y_1^q - 1$ that

$$y_2^q + (2y_1)^q = (y_2^q + 2)^2 = ((x + 3)/2)^2.$$ 

Since $q \mid x$ and $q > 3$ we see $q \mid (x + 3)/2$; thus

Received by the editors June 3, 1975.


© American Mathematical Society 1976
\[(y_2^2 + 2y_1, ((y_2^2)q + (2y_1)q)/(y_2^2 + 2y_1)) = 1,\]

by Lemma 3.

In view of (1), it follows that \(y_2^2 + 2y_1 = h^2\) where \(h|(x + 3)/2\). This gives

\[(2) \quad (hy_2)^2 + y_1^2 = (y_2^2 + y_1)^2.\]

Since \((y_1, y_2) = 1\), this implies \((hy_2, y_1) = 1\). We observe that since \(y_2\) is odd, so is \(h\); then \(4|y^2 - y_2^2\) so that \(2|y_1\).

By Lemma 2, the solutions of (2) are given by

\[hy_2 = a^2 - b^2, \quad y_1 = 2ab \quad \text{and} \quad y_2^2 + y_1 = a^2 + b^2 \quad (a > b).\]

Therefore, \((a - b)^2 = (y_2^2 + y_1) - y_1 = y_2^2\) which implies \(y_2 = a - b\), and so

\[y_1 - y_2 = 2ab - (a - b) = a(2b - 1) + b > 0, \quad \text{hence} \quad y_1 > y_2.\]

However, \(y_2^2 = 2^{q} - y_1^q - 1 > y_1^q\) implies \(y_2 > y_1\), and this is impossible. This completes Case I.

**Case II.** The proof for this case proceeds similarly. It can be easily seen from

\[(y_2^2)^q - (2y_1)^q = (y_2^4 - 2)^2 = ((x - 3)/2)^2\]

follows \(y_2^2 - 2y_1 = h^2\) where \(h|(x - 3)/2\); this implies \((hy_2)^2 + y_1^2 = (y_2^2 - y_1)^2\) so that Lemma 2 gives

\[hy_2^2 = a^2 - b^2, \quad y_1 = 2ab, \quad y_2^2 - y_1 = a^2 + b^2 \quad (a > b).\]

Hence \(y_1 - y_2 = 2ab - (a + b) = (a - 1)(b - 1) + (ab - 1) > 0\) which is impossible because of \(y_2^2 = 2^q - y_1^q + 1 > y_1^q\). This completes the proof of our Theorem.

**References**

2. ———, On the Diophantine equation \(x^n = y^n + 1, xy \neq 0\), Sci. Sinica 14 (1965), 457-460. MR 32 #1164.

**Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802**