

58. Simple Proof of Fermat's Last Theorem for $n=4$

By Yasutaka SUZUKI

Department of Mathematics, Faculty of Education,
Niigata University

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1986)

In this paper, we shall give a simple proof of the following theorem which is slightly stronger than, and implies Fermat's last theorem for $n=4$.

Theorem 1. *Let m be a non-negative integer. Then the equation*

$$x^4 + 2^m y^4 = z^4$$

has no solutions in odd integers x, y, z .

Theorem 2. *The equation $X^4 + Y^4 = Z^4$ has no solutions in positive integers.*

Proof. Let d be a greatest common divisor of X and Y . It would follow that d divided Z . Set $X=dx$, $Y=dy$, $Z=dz$. Then x and y are relatively prime. If x and y are both odd integers, since the square of an odd integer is congruent to 1 modulo 4, we have

$$x^4 + y^4 \equiv 2 \pmod{4}. \quad \text{But } z^4 \equiv 0 \pmod{4} \quad \text{or} \quad z^4 \equiv 1 \pmod{4},$$

and hence x and y must be of opposite parity and without loss of generality we may assume that y is even. Let $y=2^m y_0$ where m is a positive integer and y_0 is an odd integer. Therefore we obtain

$$x^4 + 2^{4m} y_0^4 = z^4$$

where x, y_0, z are all odd integers. Thus it is sufficient to complete the proof of this Fermat's last theorem for $n=4$ that we prove Theorem 1.

Proof of Theorem 1. Suppose that u is the least number for which $x^4 + 2^m y^4 = u^4$ has a solution in positive odd integers x, y, u for some non-negative integer m . The statement that u is least immediately implies that three integers x, y, u are pairwise relatively prime. Since the fourth power of an odd integer is congruent to 1 modulo 16, we have

$$2^m y^4 = u^4 - x^4 \equiv 1 - 1 = 0 \pmod{16}.$$

Then $m > 3$. Since u and x are both odd and relatively prime, we have

$$u^2 + x^2 \equiv 2 \pmod{4}$$

and

$$(u^2 + x^2, u+x) = (u^2 + x^2, u-x) = (u+x, u-x) = 2.$$

And since

$$2^m y^4 = u^4 - x^4 = (u-x)(u+x)(u^2 + x^2),$$

there are positive odd integers A, B, C such that

$$u-x = 2A, \quad u+x = 2^{m-2}B, \quad u^2 + x^2 = 2C$$

or

$$u-x = 2^{m-2}B, \quad u+x = 2A, \quad u^2 + x^2 = 2C.$$