Research Article

Sudhangshu B. Karmakar*

An elementary proof of Fermat's last theorem for all even exponents

DOI: 10.1515/jmc-2016-0018

Received April 4, 2016; revised August 5, 2016

Abstract: An elementary proof that the equation $x^{2n} + y^{2n} = z^{2n}$ can not have any non-zero positive integer solutions when n is an integer ≥ 2 is presented. To prove that the equation has no integer solutions it is first hypothesized that the equation has integer solutions. The absence of any integer solutions of the equation is justified by contradicting the hypothesis.

Keywords: Rational triangle, parametric solutions, Fermat's last theorem, even exponents

MSC 2010: 11D61, 11D41, 11A99, 11D99

Communicated by: Spyros S. Magliveras

Ever since the French mathematician Pierre de Fermat [2] stated the conjecture in 1637 that the equation $a^n + b^n = c^n$ cannot have solutions if a, b, c are integers > 0 and n is an integer > 2 , the equation has been a subject of intense and often heated discussions amongst mathematicians and non-mathematicians alike. This conjecture is known as Fermat's last theorem. The fact that Fermat claimed to have a proof but never wrote it down has put researchers in a quandary since nobody has yet been able to duplicate the proof Fermat originally claimed. Perhaps the strong appeal of the problem is the simplicity and elegance of its statement contrasted with the apparent hopelessness [7] of finding an elementary way to establish it. Finally, around 1994 based on a property, called modularity of an elliptic curve, Andrew Wiles [12] with the help of Taylor [11] offered a proof of the theorem. His paper incorporates by references [3, 8] a vastly larger body of mathematical work developed over the last several decades. But it requires an extraordinary arsenal [10] of mathematical tools to understand Wiles' complex and very lengthy proof. The proof vastly differs in scope and complexity from the proof Fermat originally envisioned. Consequently, the quest for a simple and short proof continues. Of course, any general proof of the theorem will also imply the proof of any special case. In this paper, based on elementary principles, a simple proof of the theorem is given for even exponents > 2 .

Theorem. *The equation*

$$x^{2n} + y^{2n} = z^{2n} \quad (1)$$

has no non-zero integer solutions when the exponent n is an integer > 1 .

Previous works. Equation (1) has been of great interest to number theorists for a long time. In 1837, E. E. Kummer [2, 9] proved that if (1) has integer solutions then $n \equiv 1 \pmod{8}$. Rothholtz [2] extended Kummer's result to prove that (1) has no integer solution if the exponent n is a prime of the form $n = 4t + 3$ or one of the variables x, y, z is a prime. In 1977, Terjanian [9] offered a surprisingly simple proof that if (1) is satisfied for non-zero integers then n divides x or y . Equivalently, Terjanian proved Fermat's last theorem for the first case with even exponents. In this paper, a simple proof of the theorem is offered for all even exponents.

*Corresponding author: Sudhangshu B. Karmakar: 33 Shirley Parkway, Piscataway, NJ 08854, USA, e-mail: math75321@gmail.com

Simplification of the theorem. Any integer > 2 is either divisible by 4 or an odd prime. Fermat's last theorem is already known to be true when n is a multiple of 3 or 4 (see [10]). Again, x, y, z must not have any common factor. Otherwise, both sides of the equation can be divided by the common factor to obtain a smaller solution. Also for consistency only one of the variables can be even. When z is even, the left-hand side of (1) is equivalent to 2 (mod 4) and the right-hand side of (1) is equivalent to 0 (mod 4). This leads to an inconsistency. Again since Fermat's equation deals with the situation where all three variables have like powers, it is enough to prove the theorem when the three variables x, y, z are relatively prime integers, y is even, the exponent n is a prime $k > 3$ and none of the variables is a prime (see [2]).

Search for integer solutions. Throughout the paper all the variables are positive integers. By $(x, y, z) = 1$ we mean that x, y, z are coprime integers and $2 \nmid y$. By $(a, b) = 1$ we mean that a, b are coprime integers and $2 \nmid b$.

Hypothesis. Fermat's equation with an even exponent has integer solutions.

Equation (1) can be written as

$$X^2 + Y^2 = Z^k, \quad (2)$$

where $X = x^k, Y = y^k, Z = z^2$.

Conditions. $(X, Y, Z) = 1, Z$ is an odd square, X, Y are k -th powers, k is a prime > 3 . Note that (2) can have integer solutions as seen from the example $41^2 + 38^2 = 5^5$. The objective here is to show that the solutions of (2) cannot be of the form $X = U^k, Y = V^k, Z = z^2$ where $(U, V, z) = 1$. Since integer solutions of (1) are assumed by using Terjanian's result [9], one notes $2k \nmid Y$.

To investigate the integer solutions of (2) under the stated conditions, we introduce two equations

$$X + iY = (g + ih)^k, \quad (3)$$

$$X - iY = (g - ih)^k \quad (4)$$

such that $(g, h) = 1$ and $2 \nmid h$ (see [1, p. 536]). From (3) we get

$$X + iY = (g^2 + h^2)^{k/2} [\cos kH + i \sin kH],$$

where $\tan H = h/g$ and $0 < H < \pi/2$. Multiplying the corresponding sides of (3) and (4), we get

$$(X^2 + Y^2) = (g^2 + h^2)^k [\cos^2(kH) + \sin^2(kH)]. \quad (5)$$

Consequently, from (5) we get

$$(X^2 + Y^2) = (g^2 + h^2)^k. \quad (6)$$

Comparing (2) and (6), we get

$$z^2 = g^2 + h^2. \quad (7)$$

Under the assumption that z, g, h are all integers > 0 , equation (7) represents a right triangle ZGH whose sides and area are integers, and z is the hypotenuse. Therefore ZGH is a rational right triangle [6]. Equivalently, (g, h, z) is a Pythagorean triple. Consequently, we get

$$X = z^k \cos(kH),$$

$$Y = z^k \sin(kH),$$

$$x = z(\cos kH)^{1/k}, \quad (8)$$

$$y = z(\sin kH)^{1/k}, \quad (9)$$

where $\tan H = h/g$ and $0 < H < \pi/2$. Substituting (8) and (9) in (1) and $n = k$, we get

$$x^{2k} + y^{2k} = z^{2k} [\cos^2(kH) + \sin^2(kH)].$$

Since $\cos^2(kH) + \sin^2(kH) = 1$, we conclude that x and y as obtained in (8) and (9) are indeed the parametric solutions of (1).

From (3) we get $X = \text{Real}[(g + ih)^k]$ and $Y = \text{Imag}[(g + ih)^k]$. Thus we get

$$X = \sum_{i=0}^j (-1)^i \binom{k}{2i} g^{k-2i} h^{2i},$$

$$Y = \sum_{i=0}^j (-1)^i \binom{k}{2i+1} g^{k-2i-1} h^{2i+1},$$

where $j = (k-1)/2$, and thus

$$X = g(g^{k-1} - C_1 g^{k-3} h^2 + C_2 g^{k-5} h^4 + \dots + (-1)^{(k+3)/2} k h^{k-1}), \quad (10)$$

$$Y = fh(h^{k-1} - C_1 h^{k-3} g^2 + C_2 h^{k-5} g^4 + \dots + (-1)^{(k+3)/2} k g^{k-1}), \quad (11)$$

where $C_1, C_2, \dots$ are integers, each divisible by k , $f = +1$ if $k \equiv 1 \pmod{4}$. Otherwise, $f = -1$. The sign of f will influence only the orientation of X and Y but will have no impact on the integer solutions of (1).

Equations (10) and (11) are rewritten as

$$X = gQ, \quad (12)$$

$$Y = hR, \quad (13)$$

respectively, where Q, R are real integers. Since $(g, h) = 1$ and $k|h$, we conclude that $(g, Q) = 1$ and $(h, R) = k$. Therefore, if X and Y are k -th powers, then g, Q, h , and R must take values of the forms

$$g = u^k, \quad Q = w^k, \quad h = k^{rk-1} v^k, \quad R = kd^k,$$

where $(u, v) = 1$, and u, r, v, d are integers > 0 , and w is an integer > 1 . From (12) and (13) we thus obtain

$$\tan kH = Y/X = (h/g)(kd^k/w^k),$$

$$\tan kH / \tan H = k(d/w)^k. \quad (14)$$

The impossibility of (14) will imply the impossibility of (1). By expanding $\tan kH$ in terms of $\tan H$ (see [5, p. 111]), we get $k(d/w)^k = U/V$, $(U, V) = 1$, $U = kd^k$, $V = w^k$, $e = h^2$, $f = g^2$. Thus we get

$$U = e^p + C_{p-1} e^{p-1} f + C_{p-2} e^{p-2} f^2 + \dots + C_1 e + C_0, \quad (15)$$

$$V = f^p + D_{p-1} f^{p-1} e + D_{p-2} f^{p-2} e^2 + \dots + D_1 f + D_0, \quad (16)$$

where the coefficients $C_0, C_1, \dots, C_{p-1}$ and $D_0, D_1, \dots, D_{p-1}$ are non-zero integers. It will be enough to prove that e is not an integer given f is an integer. This will imply that h is not an integer given g is an integer. With this assumption, equations (15) and (16) are transformed into

$$e^p + E_{p-1} e^{p-1} + E_{p-2} e^{p-2} + \dots + E_1 e + (-1)^k (f^{(k-1)/2} + kd^k) = 0, \quad (17)$$

$$f^p + F_{p-1} f^{p-1} + F_{p-2} f^{p-2} + \dots + F_1 f + (-1)^k (ke^{(k-1)/2} - w^k) = 0. \quad (18)$$

To prove that both g and h cannot be integers, it is enough to prove that at least one of (17) and (18) cannot have integer solutions.

Assertion. Both (17) and (18) cannot have integer solutions.

The coefficients $E_{p-1}, E_{p-2}, \dots$ and $F_{p-1}, F_{p-2}, \dots$ in (17) and (18) are all divisible by k . But since $(k, w) = 1$, k does not divide $(ke^{(k-1)/2} + w^k)$. By applying Eisenstein's criteria [4, pp. 160–161], it is seen that both (17) and (18) cannot be candidates for integer solutions. This justifies the assertion.

Consequently, (14) cannot be satisfied under the given conditions. Therefore, the hypothesis is contradicted. This proves Fermat's last theorem for all even exponents.

Acknowledgment: The author wishes to thank the referee for his valuable comments on the initial version of the paper which greatly helped improve upon the final presentation.

References

- [1] H. Darmon and A. Granville, On the Equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. Lond. Math. Soc.* **27** (1995), 513–543.
- [2] L. E. Dickson, *History of the Theory of Numbers. Volume II*, Washington Carnegie Institution of Washington, Washington, 1920.
- [3] Y. Hellegouarch, *Invitation to the Mathematics of Fermat–Wiles*, Academic Press, San Diego, 2002.
- [4] I. M. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, New York, 1975.
- [5] E. W. Hobson, *A Treatise on Plane Trigonometry*, Cambridge University Press, Cambridge, 1928.
- [6] D. N. Lehmer, Rational triangles, *Ann. of Math. (2)* **1** (1900), 97–102.
- [7] C. J. Mozzochi, *The Fermat Proof*, Trafford Publishing, Victoria, 2004.
- [8] A. Poorten, *Notes on Fermat's Last Theorem*, John Wiley, New York, 1996.
- [9] P. Ribenboim, *13 Lectures on Fermat's Last theorem*, Springer, New York, 1979.
- [10] K. A. Ribet and B. Hayes, Fermat's last theorem and modern arithmetic, *Amer. Sci.* **82** (1994), no. 2, 144–156.
- [11] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141** (1995), no. 3, 553–572.
- [12] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), 443–551.