An Approach to a Simple Proof of Fermat's Last Theorem

Mike Winkler
Fakultät für Mathematik, Ruhr-Universität Bochum
mike.winkler@ruhr-uni-bochum.de
www.mikewinkler.co.nf

April 2, 2018

Abstract

Fermat's Last Theorem states that the Diophantine equation $X^n + Y^n = Z^n$ has no non-trivial solution for any n greater than 2. In this paper we give an approach to a brief and simple proof of the theorem using only elementary methods.

Introduction

The only known successful proof of Fermat's Last Theorem was given in 1994 by Andrew Wiles [7]. Unfortunately this proof contains nearly hundred pages and can be understood in its entirety only by some specialists. For this reason and relating to Fermat's famous marginal note[1], many people (mostly amateurs) are still looking for a shorter and simpler proof based on elementary methods. In this paper we give an approach to such a proof.

To prove Fermat's Last Theorem it suffices to prove it for the exponent 4 and every odd prime exponent. A proof for the case $n = 4$ has already been given by Fermat himself. Therefore we give our approach only for the prime exponents greater than 2.

[1] See [6] for the complete text.

Part One

Lemma 1. *Let p, q be integers with $gcd(p, q) = 1$, then for any odd prime n there exists an integer $\lambda_{n,p,q}$ with $gcd(p, q, \lambda_{n,p,q}) = 1$ such that*

$$(p-q)^n = p^n - q^n - npq(p-q)\lambda_{n,p,q}. \tag{1}$$

Proof. According to the binomial theorem, we have

$$\begin{aligned}(p-q)^n &= \sum_{k=0}^{n} \binom{n}{k} p^{n-k}(-q)^k \\ &= p^n - q^n + \sum_{k=1}^{n-1} \binom{n}{k} p^{n-k}(-q)^k \\ &= p^n - q^n - npq \cdot \sum_{k=1}^{n-1} \frac{1}{n}\binom{n}{k} p^{n-k-1}(-q)^{k-1} \\ &= p^n - q^n - npq(p-q) \cdot \sum_{k=1}^{n-2} \frac{1}{n}\left(\binom{n-1}{k} + (-1)^{k+1}\right) p^{n-k-2}(-q)^{k-1}. \end{aligned} \tag{2}$$

The term $\frac{1}{n}\left(\binom{n-1}{k} + (-1)^{k+1}\right)$ assumes only positive integer values for and odd prime n. A proof can be found in Mamakani [3]. The OEIS reference for these values is A219539 [5].

By substituting $\lambda_{n,p,q} = \sum_{k=1}^{n-2} \frac{1}{n}\left(\binom{n-1}{k} + (-1)^{k+1}\right) p^{n-k-2}q^{k-1}$ into (2) we get (1). For $n = 3$ we have $\lambda_{3,p,q} = 1$. For primes $n > 3$ it follows from $gcd(p, q) = 1$ and the expansion of $\lambda_{n,p,q}$, given by

$$p^{n-3} - \frac{\binom{n-1}{2} - 1}{n} p^{n-4}q + \cdots - \frac{\binom{n-1}{n-3} - 1}{n} pq^{n-4} + q^{n-3}, \tag{3}$$

that $gcd(p, q, \lambda_{n,p,q}) = 1$. Because if p divides $\lambda_{n,p,q}$ then $p \mid q^{n-3}$, and if q divides $\lambda_{n,p,q}$ then $q \mid p^{n-3}$. This completes the proof. □

Remark 2. According to Lemma 1, for primes $n \geq 5$ the further factorisation of $\lambda_{n,p,q}$ is known. We have

$$\begin{aligned} (p^2 - pq + q^2) \ &\mid \lambda_{n,p,q} \quad \text{for each} \quad n \equiv -1 \pmod 6, \\ (p^2 - pq + q^2)^2 &\mid \lambda_{n,p,q} \quad \text{for each} \quad n \equiv \ \ 1 \pmod 6. \end{aligned} \tag{4}$$

For a proof we refer the reader to [1].

Lemma 3. *Let a, b, c be integers defined by*

$$a = \frac{1}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-2-k}(z^{k+1} - y^{k+1}), \tag{5}$$

$$b = \frac{1}{z-y} \cdot \sum_{k=0}^{n-1} x^{n-1-k}(z^{k+1} - y^{k+1}), \tag{6}$$

$$c = \frac{1}{z-y} \cdot \sum_{k=0}^{n} x^{n-k}(z^{k+1} - y^{k+1}), \tag{7}$$

then the identity

$$z^n = axy - b(x+y) + c, \tag{8}$$

holds for all integers x, y, z and any nonnegative integer n.

Proof. Multiplying (5) by x gives

$$ax = \frac{1}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-1-k}(z^{k+1} - y^{k+1}).$$

Adding $\frac{z^n - y^n}{z-y}$ we get

$$ax + \frac{z^n - y^n}{z-y} = \frac{1}{z-y} \cdot \sum_{k=0}^{n-1} x^{n-1-k}(z^{k+1} - y^{k+1}) = b. \tag{9}$$

Multiplying by $(z-y)$ yields

$$ax(z-y) + z^n - y^n = b(z-y). \tag{10}$$

Multiplying (6) by x we have

$$bx = \frac{1}{z-y} \cdot \sum_{k=0}^{n-1} x^{n-k}(z^{k+1} - y^{k+1}).$$

Adding $\frac{z^{n+1} - y^{n+1}}{z-y}$ we get

$$bx + \frac{z^{n+1} - y^{n+1}}{z-y} = \frac{1}{z-y} \cdot \sum_{k=0}^{n} x^{n-k}(z^{k+1} - y^{k+1}) = c. \tag{11}$$

Multiplying by $(z-y)$ we obtain

$$bx(z-y) + z^{n+1} - y^{n+1} = c(z-y). \tag{12}$$

Now we can prove the evidence of (8). Multiplying (8) by $(z-y)$ gives

$$z^n(z-y) = axy(z-y) - b(x+y)(z-y) + c(z-y).$$

Applying (10) on the right-hand side we get

$$\begin{aligned} z^n(z-y) &= y\big(b(z-y) - z^n + y^n\big) - b(x+y)(z-y) + c(z-y) \\ &= -bx(z-y) - yz^n + y^{n+1} + c(z-y). \end{aligned}$$

Applying (12) on the right-hand side yields

$$\begin{aligned} z^n(z-y) &= -bx(z-y) - yz^n + y^{n+1} + bx(z-y) + z^{n+1} - y^{n+1} \\ &= z^{n+1} - yz^n. \end{aligned}$$

We obtain a true statement, which completes the proof. □

Theorem 4. *The Diophantine equation $X^n + Y^n = Z^n$ has no non-trivial solution for any odd prime number n.*

Proof. We assume that x, y, z are nonzero integers and n is an odd prime such that

$$x^n + y^n = z^n. \tag{13}$$

It suffices to consider only solutions (x, y, z) with $gcd(x, y, z) = 1$. Hence x, y, z are pairwise relatively prime and exactly one of these integers is even. Applying Lemma 1 with $p = z$, $q = x + y$, we have

$$(z - x - y)^n = z^n - (x + y)^n - n(x + y)z(z - x - y)\lambda_{n,z,x+y}.$$

Applying Lemma 1 with $p = x$, $q = -y$, on the right-hand side gives

$$(z - x - y)^n = z^n - x^n - y^n - nxy(x + y)\lambda_{n,x,-y} - n(x + y)z(z - x - y)\lambda_{n,z,x+y}.$$

Applying (13) on the right-hand side we obtain

$$(z - x - y)^n = -nxy(x + y)\lambda_{n,x,-y} - n(x + y)z(z - x - y)\lambda_{n,z,x+y},$$

that is

$$(z - x - y)^n = n(x + y)\big(xy\lambda_{n,x,-y} - z(z - x - y)\lambda_{n,z,x+y}\big). \tag{14}$$

Because n is an odd prime we conclude from (14) that $n \mid (z-x-y)^n$, hence $n \mid (z-x-y)$. Dividing (14) by n^2 it follows that n divides $(x+y)$ or $\big(xy\lambda_{n,x,-y} - z(z-x-y)\lambda_{n,z,x+y}\big)$. From (13) we conclude that $(x + y) \mid z^n$, hence if n divides $(x + y)$ then $n \mid z$. If n divides $\big(xy\lambda_{n,x,-y} - z(z - x - y)\lambda_{n,z,x+y}\big)$ then $n \mid xy\lambda_{n,x,-y}$, because $n \mid (z - x - y)$. It follows from $gcd(x, y, \lambda_{n,x,-y}) = 1$ that n divides one and only one of the integers x, y, or $\lambda_{n,x,-y}$. So we have to consider two cases. *Case* 1: If $n \nmid \lambda_{n,x,-y}$ then $n \mid xyz$. By $gcd(x, y, z) = 1$ it follows that n divides one and only one of the integers x, y, z. *Case* 2: If $n \mid \lambda_{n,x,-y}$ then $n \nmid xyz$. This applies if and only if n is congruent 1 (mod 6) or an exceptional prime as listed in A068209 [4]. Unfortunately, it is an open problem if there exists a simple method of characterizing these exceptional primes.

Applying Lemma 1 with $p = z$, $q = y$, it follows from (13) that

$$\frac{x^n}{z - y} = (z - y)^{n-1} + nzy\lambda_{n,z,y}. \tag{15}$$

Now we assume that $x \neq \pm 1$ and $n \nmid x$. From (15) we conclude that $(z - y) \mid x^n$, hence $n \nmid (z - y)$. Now we consider two cases. *Case* 1: If x is even then y, z are odd, so $(z - y)$ is even. Applying Lemma 1 it follows from (3) that $\lambda_{n,z,y}$ consists of an odd number of terms, where the number of even coefficients is even and the number of odd coefficients is odd. Hence, with y, z odd, $\lambda_{n,z,y}$ is a sum of an odd number of odd terms and an even number of even terms, so $\lambda_{n,z,y}$ is odd. *Case* 2: If x is odd then y, z have different parity, so $(z - y)$ is odd. Applying Lemma 1 it follows from (3) with y or z even that each term of $\lambda_{n,z,y}$ is even except $(z^{n-3} + y^{n-3})$ which is odd, so $\lambda_{n,z,y}$ is odd. From $gcd(z, y) = 1$ we have $gcd(z, y, z - y) = 1$, hence $gcd(z - y, \lambda_{n,z,y}) = 1$, so $gcd(z - y, zy\lambda_{n,z,y}) = 1$. Therefore a prime factor of x and $(z - y)$ does not divide the right-hand side of (15), which clearly forces that $(z - y)$ is an n-th power. It follows

that there exist integers u, v with $gcd(u, v) = 1$ such that $x = uv$ and $z - y = u^n$ and $v \nmid (z - y)$.

Applying (13) on the right-hand side of (10) we obtain $ax(z - y) + x^n = b(z - y)$, which gives

$$x^n = (b - ax)(z - y). \tag{16}$$

Substituting $x = uv$ and $z - y = u^n$ into (16) gives $(uv)^n = (b - auv)u^n$, hence

$$v^n = b - auv = b - ax. \tag{17}$$

It follows from (17) that $v \mid b$, and consequently from (8) and $gcd(x, y, z) = 1$ that $v \nmid c$. According to Lemma 3 we can show by a similar proof that $x^n = ayz - b(y + z) + c$, which yields with $v \mid x$, $v \mid b$, $v \nmid c$ and $gcd(x, y, z) = 1$ that $v \nmid a$. With $gcd(u, v) = 1$ and $v \mid b$, $v \nmid a$ it follows from (17) that $v^2 \nmid b$. Substituting $z - y = u^n$ into (12) we obtain $bxu^n + z^{n+1} - y^{n+1} = cu^n$, which gives

$$\frac{z^{n+1} - y^{n+1}}{c - bx} = u^n. \tag{18}$$

...

□

Remark 5. The terms from (5)–(7) represent special cases of the trinomial expansion of $(x+y+z)^n$ with the peculiarity that all trinomial coefficients given by $\binom{n}{i,j,k} = \frac{n!}{i!\,j!\,k!}$ were set equal to 1. Let x, y, z be integers, then for any nonnegative integer n we have

$$\frac{1}{z-y} \cdot \sum_{k=0}^{n} x^{n-k}(z^{k+1} - y^{k+1}) = \sum_{i+j+k=n} x^i y^j z^k,$$

where i, j, k are all nonnegative integers such that $i + j + k = n$.

Remark 6. We can rewrite the terms from (5)–(7) as fractions. From (5) we obtain

$$a = \frac{z}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-2-k} z^k - \frac{y}{z-y} \cdot \sum_{k=0}^{n-2} x^{n-2-k} y^k$$

$$= \frac{z}{z-y} \cdot \frac{z^{n-1} - x^{n-1}}{z-x} - \frac{y}{z-y} \cdot \frac{y^{n-1} - x^{n-1}}{y-x}$$

$$= \frac{x^n(z-y) + y^n(x-z) + z^n(y-x)}{(z-y)(x-z)(x-y)}$$

$$= \frac{x^n(z-y) + y^n(x-z) + z^n(y-x)}{x^2(z-y) + y^2(x-z) + z^2(y-x)}.$$

In a similar way, we may show that

$$b = \frac{x^{n+1}(z-y) + y^{n+1}(x-z) + z^{n+1}(y-x)}{x^2(z-y) + y^2(x-z) + z^2(y-x)},$$

$$c = \frac{x^{n+2}(z-y) + y^{n+2}(x-z) + z^{n+2}(y-x)}{x^2(z-y) + y^2(x-z) + z^2(y-x)}.$$

Table 1 gives an overview on all possible integer values for a, b, c from (5)–(7) for any nonnegative integer n.

n	a	b	c
0	0	0	1
1	0	1	$\in \mathbb{Z}$
2	1	$\in \mathbb{Z}$	$\in \mathbb{N}$
odd ≥ 3	$\in \mathbb{Z}$	$\in \mathbb{N}$	$\in \mathbb{Z}$
even ≥ 4	$\in \mathbb{N}$	$\in \mathbb{Z}$	$\in \mathbb{N}$

Table 1: Possible values for a, b, c.

Part Two

Acknowledgements

The author wishes to express his thanks to Andreas Fillipi. Without his contribution in a mathematics forum, I probably would never have worked on this topic again [2].

References

[1] Brown, Kenneth S.: *Sums of Powers in Terms of Symmetric Functions*, web document. (mathpages.com/home/kmath097.htm)

[2] Fillipi, Andreas: *Beitrag im Forum Elementare Zahlentheorie*, February 9, 2015, www.matheplanet.de. (tinyurl.com/y8jh4dvr)

[3] K. Mamakani, F. Ruskey, *New roses: simple symmetric Venn diagrams with 11 and 13 curves*, Disc. Comp. Geom., 52 (2014), pp. 71–87, Lemma 2.

[4] The On-Line Encyclopedia of Integer Sequences: *Considering the congruence (x+1)ˆp-xˆp=1 (mod pˆ2) sequence gives values of p of the form 3k-1 such there exist nontrivial solutions (x other than 0 or -1 modulo p)*, A068209.

[5] The On-Line Encyclopedia of Integer Sequences: *T(n,k) is the number of k-points on the left side of a crosscut of simple symmetric n-Venn diagram*, A219539.

[6] Wikipedia, *Fermat's Last Theorem*, 2.2 Fermat's conjecture. (tinyurl.com/y9hwwdb5)

[7] Wiles, Andrew: *Modular Elliptic Curves and Fermat's last theorem*, Annals of Mathematics 142 (1995), pp. 443-551.