Direct Proof of Fermat's Last Theorem Based on Induction on z Not on n

Mohamed Azzedine

Abstract: Direct proof of fermat's Last Theorem (x^n +y^n =z^n)based on Induction on z not on n. it is short, direct and comprehensible by student in Mathematics and lovers of Mathematics. It use mathematical tools of Fermat's era.

The French mathematician Pierre de Fermat (1601-1665), conjectured that the equation x^n +y^n =z^n has no solution in positive integers x, y and z if n is a positive integer >= 3. He wrote in the margin of his personal copy of Brachet's translation of Diophantus' Arithmetica:"I have discovered a truly marvellous demonstration of this proposition that this margin is too narrow to contain".
Many researchers believe that Fermat does not find a demonstration of his proposition but some others think there is a proof and Fermat's claim seems right.
The search of a solution of equation x^n + y^n =z^n are splitted in two directions.
The first one is oriented to search a solution for a specific value of the exponent n and the second is more general, oriented to find a solution for any value of the exponent n.

- Babylonian (570,495 BC) studied the equation x^2+y^2=z^2 and found the solution (3,4,5).
- Arabic mathematician Al-Khazin studied the equation x^3+y^3=z^3 in the X century and his work mentioned in a philosophic book by Avicenne in the XI century.
- A defective proof of FLT was given before 972 by the Arab Alkhodjandi
- The Arab Mohamed Beha Eddin ben Alhossain (1547-1622) listed among the problems remaining unsolved from former times that to divide a cube into two cubes.(refer Image of Arabic manuscript from British Museum. Problem N4 Red color at line 8 from top).
- Fermat (1601, 1665), Euler (1707, 1783) and Dirichlet (around 1825) solved the equation for n=3, 4 and 5.
- In 1753, Leonhard Euler presented a proof for x^3+y^3=z^3
- Fermat found a proof of x^4 +y^4 =z^4 using his famous "infinite descente". This method combines proof by contradiction and proof by backward induction.
- Dirichlet (in 1825) solved the equation x^5+y^5=z^5 .
- Sophie Germain (in 1823) generalized the result of Dirichlet for prime p if 2p+1 is prime.. Let p prime, x^p +y^p =z^p has no solution in positive integers if 2p+1 is prime.
- In XIX century E.Kummer continued the work of Gauss and innovated by using numbers of cyclotomic field and introduced the concept of "prime factor ideal".
-Andrew Wiles, a professor at Princeton University, provided an indirect proof of Fermat's Conjecture in two articles published in the May 1995 issue of Annals of Mathematics.
Andrew Wiles solved a high level problem in modular forms about elliptic curves and **the consequence is a solution for FLT. Thanks to the results of Andrew Wiles, we know that Fermat's Last Theorem is true.**
I think he opens a space for mathematicians to search proofs for FLT comprehensible by a normal student in mathematics and may be to find new concepts or ideas. **This result should imply a direct proof of FLT.**

In this paper, I would like to suggest a direct proof using mathematical concepts (Forward Induction and Backward Induction) and tools of the Fermat's era; valid for whatever value n > 2. This direct proof is comprehensible for a normal student and mathematical lovers.

I- Proof by Forward Induction :

The induction proof is on z not on n.
The induction proof starts from z =2 and z =3, z =4 … until z=p. with n>2

Observe that for $z=2$, the equation $\mathbf{x^n + y^n = 2^n}$ has no solutions in integers x and y if $n > 2$.
There is no equality between the sum (x^n+y^n) and 2^n. if $n >2$.

The case $x=y$ gives $2x^n=z^n$ which leads to $z=\mathrm{sqrt}(2)*x$ which is not an integer.

Hence x is different from y.

A. Basis step / anchoring

Let's assume $z=3$ with $1<=x < y < z$ and $x^n+y^n =3^n$

The cells of the table below show the different values of the sum (x^n+y^n) when x and y varies from 1 to 3 .

The cells of the last line show the value of $z^n=(Max(x) +1)^n=(2+1)^n=3^n$.

x^n	1	2^n	3^n
y^n			
1	1+1	$2^n +1$	$1+3^n$
2^n		2^n+2^n	$2^n +3^n$
3^n			$3^n +3^n$
z^n	3^n	3^n	

It is obvious that x^n+y^n is never equal to $z^n=(Max(x)+1)^n=(2+1)^n=3^n$.

All the sums are:

$1+1=2 < 3^n$; $1+2^n < 3^n$; and $2^n +2^n < 3^n$

The basis case with $z = 3$ does not need any proof, because you can calculate that regardless of what you choose for x, y, with $n > 2$. **The sum $(x^n + y^n)$ is either less than z^n or greater than z^n but never equal to z^n.**

Let $f(t) =3^n -(2^n +t^n)$ with $1<= t <=3$. $f(t)$ is continuous on the interval [1,3]

$f(1)=3^n - (2^n +1^n) >0$

$f(2) = 3^n - (2^n +2^n) >0$

$f(3) = 3^n -(2^n +3^n) <0$

So, as the value of t moves between 2 and 3, the value $2^n + t^n$ goes from being smaller than 3^n to being greater than 3^n. There is a change of sign of $f(t)$ in the interval [2,3]. Thus, there must be some value of t in the interval [2, 3] for which $\mathbf{2^n +t^n = 3^n}$.. The Intermediate Value Theorem (IVT) which states that « if a function is continuous on [a, b], and if L is any number between f(a) and f(b), then there must **be a value, x = c**, where a < c < b, such that f(c) = L »,. confirms our conclusion and we get

$t^n = 3^n - 2^n$ if $n=3$ we get $3 \log t = \log (27 - 8) = \log 19$ so $t=2,668$

$t = 2,668$ in the interval $[2,3]$: $2 < 2,668 < 3$

$n=3$ $\quad 2^3 + (2,668)^3 = 3^3$ or $8+19=27$

We can repeat the same process for any value of n and compute the right value of t (or y) in the interval [2, 3] in order to get $x^n + y^n = z^n$ but y is a real value not integer. x and z remain integer.

$n=2$ $\quad 2^2 + (2,236)^2 = 3^2$ or $4 + 5 = 9$

$n=4$ $\quad 2^4 + (2,839)^4 = 3^4$ or $16 + 65 = 81$

and so on

This method will be used later in Inductive step to show that t**he sum ($x^n + y^n$) is either less than z^n or greater than z^n but never equal to z^n.**

B. inductive step:

Now assume the Fermat's conjecture is true until z=p.

We know that every equation $x^n + y^n = z^n$ from z=2 and z=3 until z=p has no solutions in integers x and y if n > 2.

We want to prove that FLT is true for z=p+1.

The cells of the table below show the different values of the sum (x^n+y^n) when x and y varies from 1 to p.

The last line shows the value of z^n.

x^n	1	2^n	3^n	4^n			$(p-1)^n$	p^n
y^n								
1	1+1	2^n+1	3^n+1	4^n+1				p^n+1
2^n		2^n+2^n	3^n+2^n	4^n+2^n				p^n+2^n
3^n			3^n+3^n	4^n+3^n				p^n+3^n
4^n				4^n+4^n				p^n+4^n
					…			
						$(p-2)^n+(p-2)^n$		$p^n+(p-2)^n$
$(p-1)^n$							…	$p^n+(p-1)^n$
p^n								p^n+p^n
z^n	p^n	p^n	p^n	p^n				p^n

In the above table (**first row**=nth-powers of integer x, **first column**=nth-powers of integer y).
Each cell contains the sum (x^n+y^n).
The last row contains the value of $z^n=p^n$.

Assume Fermat's conjecture is true until $z=p$.

All the sum (x^n+y^n) are not equal to p^n .For all integers values of x and y if $n>2$ the sum $(x^n + y^n)$ is either less than p^n or greater than p^n:

If **$x^n+y^n < p^n$ then $(x^n + y^n) < p^n < (p+1)^n$.**

It is OK for FLT with $z=p+1$

If $x^n+y^n > p^n$ then there are two cases:

- **$(x^n + y^n) < (p+1)^n$ or $(x^n+y^n) > (p+1)^n$.**
- **It is OK for FLT with $z=p+1$.**

We have to prove that $(x^n +y^n)$ is never equal to $(p+1)^n$, because we already know that all the sum (x^n+y^n) are not equal to p^n .

In the last column Max(x)=p all the sum $(p^n +y^n)$ with $1 <y < p$ are either less than $(p+1)^n$ or greater than $(p+1)^n$. We have to show that there is no equality between the sum (x^n+y^n) and $(p+1)^n$.

- $p^n +1^n < (p+1)^n$
- $p^n +2^n < (p+1)^n$
- $p^n +3^n < (p+1)^n$
- ….
- **$p^n +t^n < (p+1)^n$**
- **$p^n + (t +1)^n > (p+1)^n$**
- ……
- $p^n +p^n > (p+1)^n$ with the condition $\log(1+1/p) < (\log 2) /n$
-
- With n fixed we can compute p in order to get $2*p^n > (p+1)^n$

n1	1	2	3	4	5	6
p	p=1 $\log(1+1/2)<2$ $2*1^1 \geq (1+1)^1$ $2 \geq 2$	p=3 $\log(1+1/3)<2/2$ $2*3^2>(3+1)^2$ 18>16	p=4 $\log 1+1/4)<2/3$ $2*4^3>(4+1)^3$ 128>125	p=5 $\log(1+1/6)<2/6$ $2*6^4>(6+1)^4$ 2592>2401	p=7 $\log(1+1/7)<2/7$ $2*7^5<(7+1)^5$ 33614>32768	p=9 $\log(1+1/9)<2/9$ $2*9^6>(9+1)^6$ $1062882>10^6$

So,as the variable t moves between t and t+1, the value $p^n +t^n$ goes from being lesser than $(p+1)^n$ to being greater to $(p+1)^n$. There is a change of sign. Thus, there must be some value of t in the interval [t,t+1] for which $p^n +t^n =(p+1)^n$. This is the common sense but there is actually a mathematical theorem, known as the Intermediate Value Theorem, which confirms our conclusion.

Summary. The Intermediate Value Theorem (IVT) is a precise mathematical statement (theorem) concerning the properties of continuous functions. The IVT states that if a function is continuous on $[a, b]$, and if L is any number between $f(a)$ and $f(b)$, then there must **be a value, $t = c$**, where $a < c < b$, such that $f(c) = L$.

The expression $p^n + t^n$ with $1<t<p$ starts less than $(p+1)^n$. It increases when t increases and becomes close to $(p+1)^n$. When t reaches some integer value $(p^n +t^n)$ becomes greater than $(p+1)^n$. Change of value occurs between t and $t+1$. The expression $(p^n +t^n)$ may be equal to $(p+1)^n$ with t irrational but never with t integer. There is no integer value between t and $t+1$.

Thus, there must be some value of t in the interval $[t,t+1]$ for which

$$p^n +(T)^n = (p+1)^n$$

and again, since $T >2$, this must be an irrational value.

Thus, since there are infinitely many increasing triples (x,y,z), there are infinitely many irrational values of T for which there is a solution to $x^n +y^n =z^n$.

Let the function $G(t) = (p+1)^n – p^n –t^n$ with $1\leq t \leq p$, p is fixed

The derivative is $G'(t) = - n t^{(n-1)}$. It is always negative then $G(t)$ is decreasing from a positive value $G(1)=(p+1)^n –p^n -1$ to a negative value $G(p)=(p+1)^n - (p)^n –p^n$ because $2*p^n > (p+1)^n$ as showed above.

Change of sign of $G(t)$ occurs between t and $t+1$. The expression $(p^n +t^n)$ may be equal to $(p+1)^n$ with t irrational but never with t integer. There is no integer value between t and $t+1$.

In particular, note that if $x=y$ then $x^n +y^n =z^n$ becomes $2x^n=z^n$ or $2=(z/x)^n$.

If we take now log to the base (z/x) (written $\log (z/x)$ of ( )); we get

$\log (z/x)$ of $(2)= \log(z/x)$ of $((z/x)^n)=n \log(z/x)$ of $(z/x)=n$. which is not integer.

Example, we see that

$t^n +t^n = 4^n$ when $\log t=\log 4 –1/n \log (2)$ which is real

if $n=3$ then $\log t =\log 4 -1/3 \log2$

$3^n +3^n = 4^n$ when $n=\log4/3 (2) =2,40942$ then Fermat is not true with exponent $n=$ real

All the sums (x^n+y^n) are less than $(p+1)^n$ or greater than $(p+1)^n$ and $(x^n +y^n)$ is not equal to $(p+1)^n$ for all x, y and $n>2$.

FLT is true until $z=p$ implies FLT is true for $z=p+1$

C. Conclusion

With the principle of strong mathematical induction, we can then conclude that the equation

$x^n+y^n=p^n$ has no solutions in positive integers x, y and p if $n > 2$.

This proof based on Induction on z not on n, is short, direct, comprehensible by any student in Mathematics and lovers of Mathematics.

Mohamed.AZZEDINE **October 15, 2021**
azzedine.hamed@gmail.com