# • Direct proof of Fermat's Last Theorem based on parity odd or even of numbers.

Mohamed Azzedine

Abstract: This is a Direct proof of Fermat's Last Theorem based on Even/Odd parity of numbers. It is short,direct and comprehensible by student in Mathematics and lovers of Mathematics.

# Introduction

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 (Parity Even/Odd of numbers, 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.

# Proof Of FLT:

Let we recall the Pythagorean theorem which states that x^2 +y^2 =z^2 has many integer solutions .

x= u^2 –v^2 ; y=2uv and z= u^2+v^2 with u and v positive integers, relatively prime , of opposite parity and u > v > 0.

Assume the equation x^n + y^n =z^n with x, y, z positive integers and n is integer greater than 2. .

In this proof we only deal with primitive triples which have no common divisor.

- (x^n+y^n)=(x+y)*(x^(n-1) –x^(n-2)y+………..y^(n-1))=z *z^(n-1)
- The sum (x+y) from LHS and the number z from RHS must not have any common divisor (like 2n or another) otherwise the equation x^n+y^n=z^n would be transformed in another equation degree (n-1) and different from x^n+y^n =z^n
- No two numbers from (x, y, z) can be even because two would be a common divisor.
- All three numbers (x,y,z) cannot be odd because the equation x^n +y^n =z^n would say the sum of two odd numbers is odd. Therefore, exactly one is even.
- There are 3 cases :
  - z even and x odd and y odd
  - x odd, y even and z odd
  - x even and y odd and z odd

We have to choose the right one according to the equation x^n +y^n =z^n.

## 2/ Parity table

A parity table is a mathematical table used in logic specifically in connection with parity which sets out the functional values of logical expressions ($x^n + y^n = z^n$) on each of their functional arguments, that is, for each combination of values taken by their logical variables

The cell contains the parity of each element (x,y,z) and the last column the sum ($x^n + y^n$) and the right comment.

E= Even and O=Odd

| N° | x | x^n | y | y^n | z | z^n | x^n+y^n=z^n | Comment |
|---|---|---|---|---|---|---|---|---|
| 1 | E | E | E | E | E | E | E +E=E | Excluded |
| 2 | E | E | E | E | O | O | E+E=O | Impossible |
| 3 | E | E | O | O | E | E | E +O=E | Impossible |
| 4 | E | E | O | O | O | O | E + O=O | To be examined |
| 5 | O | O | E | E | E | E | O +E=E | Impossible |
| 6 | O | O | E | E | O | O | O +E=O | To be examined |
| 7 | O | O | O | O | O | O | O +O =O | Excluded |
| 8 | O | O | O | O | E | E | O +O=E | To be examined |

## 1/ We want to prove that z is odd and x and y are of opposite parity.

If z is even then $z=2p$ with p integer . . The numbers x and y are odd and can be written as $x=2q+1$ and $y= 2r+1$..

$x^n= (2q+1)^n =(2q)^n +1 + \sum n ! / (j ! (n-j) !) (2q)^j$ with $1\leq j \leq (n-1)$

$(2q+1)^n=(2q)^n +n (2q)^{(n-1)}+n(n-1)/2 (2q)^{(n-2)}+\ldots\ldots.n(n-1)/2 (2q)^2 +n(2q) +1$

n is common factorn in all terms of binomial formula except in the leading term $(2q)^n$ and the last term (one).

$y^n =(2r)^n +1 + \sum n ! / (j ! (n-j) !) (2r)^j$

and $z^n = (2p)^n$.

If $x^n +y^n =z^n$ and z even this implies :

$[(2q)^n +1 +\sum n ! / (j ! (n-j) !) (2q)^j ] + [(2r)^n+1 +\sum n ! / (j ! (n-j) !) (2r)^j ]= (2p)^n$ with $n>2$ and $1\leq j \leq (n-1)$

# 1.1/ Suppose n=2k with k>1

$x^n= (2q+1)^n =(2q)^n +1 + \sum n ! /(j ! (n-j) !) (2q)^j$

$(2q+1)^{2k}=(2q)^{2k} +1+ \sum (2k)! /(j ! (2k-j) !) (2q)^j$

$(2q+1)^{2k} =2^{2k} q^{2k} +1 + (2k)*2 \sum (2k-1) !/(j! ( (2k-j) !) 2^{(j-1)} (q)^j$

$2^{2k} q^{2k}=4^k q^{2k}$ and $2k*2=4k$

$(2p)^{2k} =2^{2k} p^{2k} =4^k p^{2k}$

The number 4 is common divisor of $x^{2k}$, $y^{2k}$ and $z^{2k}$

$(2q+1)^{2k}=[4^k q^{2k}+4k \sum (2k-1)!/(j!((2k-j)!) 2^{(j-1)} (q)^j) +1]=4[4^{(k-1)} q^{2k} +k*Q]+1$

with Q is polynomial in q

$(2r+1)^{2k}=[4^k r^{2k}+4k \sum (2k-1)!/(j!((2k-j)!) 2^{(j-1)} (r)^j) +1]=4[4^{(k-1)} r^{2k} +k*R]+1$,

with R is polynomial in r

$(2p)^{2k} =2^{2k} p^{2k}=4[4^{(k-1)} p^{2k}]$ ,

If $x^n +y^n =z^n$ and z even this implies :

$4[4^{(k-1)}q^{2k} +k*Q +4^{(k-1)} r^{2k} +k*R] +2 =4[4^{(k-1)} (p^{2k})]$

$4[4^{(k-1)} (q^{2k} + r^{2k} -p^{2k})+ k*(Q +R)]= -2$

4 divides the LHS and must divide the RHS, thus 4 divides 2 which is a contradiction . Therefore x and y can not both be odd. Thus exactely one must be even and z must be odd

If $(q^{(2k)} + r^{(2k)} - p^{(2k)})$ is equal zero then 4 divides the LHS and must divide the RHS, thus 4 divides 2 which is a contradiction. We can infer that $(q^{(2k)} + r^{(2k)} - p^{(2k)})$ cannot equal zero and FLT is true for n even equal 2k with k>1

## 1.2/ Suppose n=2k+1 with k>0

$x^n= (2q+1)^n =(2q)^n +1 + \sum n!/(j!(n-j)!) (2q)^j$

$(2q+1)^{2k+1}=(2q)^{(2k+1)} +1+ \sum (2k+1)!/(j!(2k+1-j)!) (2q)^j =2^{(2k+1)} q^{(2k+1)} +1 + (2k+1)*(2) \sum (2k)!/(j!((2k+1-j)!) 2^{(j-1)} (q)^j$

The number 4k+2 is common divisor of binomial terms except the term 1.
$(2q+1)^{(2k+1)}=(4k+2)*Q +1 +(2q)^{(2k+1)}$, Q is polynomial in q

$(2r+1)^{(2k+1)} = (4k+2)*R +1 + (2r)^{(2k+1)}$, R is polynomial in r

If $x^n +y^n =z^n$ and z even this implies

$(4k+2)*Q +1 + (2q)^{(2k+1)} +(4k+2)*R +1 +(2r)^{(2k+1)} =2^{(2k+1)}p^{(2k+1)}$

$(4k+2)*(Q +R )=-2 [1 + 2^{2k} (q^{(2k+1)} + r^{(2k+1)} -p^{(2k+1)})]$

4k+2 divides the LHS and must divide the RHS, thus 4k+2 divides 2 which is a contradiction or divides $(1+2^{2k} (q^{(2k+1)} + r^{(2k+1)} - p^{(2k+1)}))$ which is an odd number .4k+2 cannot divides it because 4k+2 is even. Therefore x and y can not both be odd. Thus exactely one must be even and z must be odd.

If $(q^{(2k+1)} + r^{(2k+1)} - p^{(2k+1)})$ is equal zero then 4k+2 divides the LHS and must divide the RHS, thus 4k+2 divides 2 which is a contradiction. . We can infer that $(q^{(2k+1)} + r^{(2k+1)} - p^{(2k+1)})$ cannot equal zero and FLT is true for n odd equal 2k+1 with k>0.

**The two cases n=2k or n=2k+1 yields to contradiction.This contradiction proves that z is odd .Assume that y is the other odd number if it is not then switch with x because x and y are interchangeable in the equation x^n +y^n =z^n.**

**So z is odd  x, and y are of opposite parity.**

**Summary Parity table**

| X | Even | | Odd | |
|---|---|---|---|---|
| Y | | | | |
| Even | Even+Even=Even | Excluded | Odd+Even=Odd | To be examined |
| | Even+Even=Odd | Impossible | Odd+Even=Even | Impossible |
| | | | | |
| Odd | Even +Odd =Odd | To be xamined | Odd + Odd =Odd | Excluded |
| | Even +Odd =Even | impossible | Odd + Odd =Even | To be examined |

**2.1/ We will examine the case Odd +Odd= Even.**

Assume x=2q+1, y=2r+1 and z=2p

x^n+y^n =z^n

(2q+1)^n +(2r+1)^n =(2p)^n

((2q+1) +(2r+1))*[(2q+1)^(n-1) –(2q+1)^(n-2) (2r+1)+…..(2r+1)^(n-1)]=(2p)^n

((2q+1) +(2r+1))=2(q+r+1) is even

(2p) is also even. These two terms has 2 as a common factor, so the equation is excluded because it does not a Fermat's equation.

3.1/ **We will examine now the 2 cases  Even + Odd =Odd  and**

**Odd + Even = Odd**

Assume x odd, y even and z odd
y^n=z^n - x^n
y^n = z^n - x^n =(z-x) [z^(n-1) +x z^(n-2)+.........+x^(n-1)]
y^n is even, (z-x) is even and [z^(n-1) +x z^(n-2)+.........+x^(n-1)] is the product of module of all complex roots .

## 3.1.1/ If n is even , n=2m

z^n –x^n= (z^2 –x^2) ∏ (z^2 -2zx cos(2k*pi)/n +x^2) with 1≤ k ≤ (m-1)

z^n –x^n= (z^2 –x^2)*Product of module of complex roots from k=1 to k=m-1.

We can write y=2p ; (z-x) =2q and z+x=2r and [z^(n-1) +x z^(n-2)+.........+x^(n-1)]=Product of module=∏ (Mi)^2

with p, q and r integers because y,is even and (z-x) is even and z+x=2r and [z^(n-1) +x z^(n-2)+.........+x^(n-1)]= ∏ (Mi)^2..
Plug these values into y^n =z^n - x^n it becomes y^n=(2p)^n =(2q) (2r) ∏ (Mi)^2.

We get y = 4^(1/n) (qr)^(1/n) (∏ (Mi)^2)^(1/n) .

Due to irrationality of 4^(1/n) and (∏ (Mi)^2)^(1/n) we cannot get y is an integer with n>2.
This is a contradiction according to the premise.( y is integer and even)

**Checking for n=2,** x^2 +y^2 =z^2

y^2=z^2- x^2 = (z-x)(z+x)

Assume x odd, y even and z odd

We can write y=2p ; (z-x) =2q and z+x=2r

with p, q and r integers because y,is even and (z-x) is even and z+x is even .
Plug these values into y^2 =z^2 - x^2 it becomes y^2=(2p)^2 =(2q) (2r)

We get p^2 =qr with q and r coprime . Since qr=p^2 we know that q and r must each be square

This implies there exist q=v^2 and r=u^2. We get y^2=2u^2 *2v^2 and z-x=2v^2 and z+x=2u^2

We get x=u^2 –v^2 , y=2uv, z=u^2+v^2. We find the well known pythagorean solution for the equation x^2+y^2=z^2.

## 3.1.2/ If n is odd , n=2m+1

z^n –x^n= (z –x) ∏ (z^2 -2zx cos(2k*pi)/n +x^2) with 1≤ k ≤ m

z^n –x^n= (z –x)*Product of module of complex roots from k=1 to k=m.

z^n –x^n= (z –x)*Product of module of complex roots from k=1 to k=m.

We can write y=2p ; (z-x) =2q and [z^(n-1) +x z^(n-2)+.........+x^(n-1)]=Product of module=∏ (Mi)^2
with p, q integers because y,is even and (z-x) is even and [z^(n-1) +x z^(n-2)+........+x^(n-1)]= ∏ (Mi)^2..
Plug these values into y^n =z^n - x^n it becomes y^n=(2p)^n =(2q) ∏ (Mi)^2.

We get y=2^(1/n) q^(1/n) (∏ (Mi)^2)^(1/n) .

Due to irrationality of 2^(1/n) we cannot get y as an integer.

This is a contradiction according to the premise.( y is integer and even)

We can claim that the parity combination odd +even =odd is impossible.

In the equation x^n +y^n =z^n the variables x and y are interchangeable.

We can replace x by y in the demonstration above and we get the parity combination

even +odd = odd is impossible.

**Cheking with n=3 ,** $x^3+y^3=z^3$

$y^3=z^3 - x^3=(z-x) (z^2 +xz +x^2)$

Assume x odd, y even and z odd

We can write $y=2p$ ; $(z-x) =2q$ and $z^2+xy +x^2=(z^2 +2 (x z) 1/2 +x^2)= (z^2 -2 (x z) \cos (120°) +x^2)=M^2$ (M as module of complex root)

with p, q integers because y,is even and (z-x) is even .
Plug these values into $y^3 =z^3 - x^3$ it becomes $y^3= (2p)^3 =(2q) (M^2)$

$y^3=(2q) (M^2)$ or $y=2^{(1/3)} q^{(1/3)} M^{(2/3)}$ which is not an integer, due to irrationality of $2^{(1/3)}$.

This is a contradiction according to the premise. (y is integer and even).

We can claim that the parity combination odd +even =odd is impossible.

In the equation $x^3+y^3=z^3$ the variables x and y are interchangeable. The parity combination even + odd =odd is also impossible if we replace x by y in the demonstration above..

## 4/ Conclusion

**All the parity combinations of x, y and z are examined and eliminated.**

**So Fermat's Last Theorem is always true.**
**In all cases the equation $x^n +y^n =z^n$ is impossible and we can claim that**

**$x^n +y^n =z^n$ has no integer solutions for n>2.**

Q.E.D

# III. References:


[1] A. Wiles, Modular elliptic curves and Fermat's Last Theorem. *Annals Math*., 142 (1955), 443-451.

[2] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Annals Math*., 142 (1955), 553-572.

[3] P. Ribenboim, *Fermat's Last Theorem*, Springer-Verlag, New York, 1999.

[4] D.M.Burton, *Elementary Number Theory*, Fifth Edition, Mc Graw-Hill, New York, 2002.

[5] B. Poonen, *Some Diophantine equations of the form x^n+y^n=z^m*, Acta Arith, 86 (1955)

[6] Gareth A.Jones and J.Mary Jones (2005). Elementary Number Theory. Springer

[7] A proof of Fermat's Last Theorem using an Euler's Equatio. Available from:

https://www.researchgate.net/publication/319934410

[8] Inductive reasoning. http://en.wikipedia.org/wiki/Inductive_reasoning Wikipedia [retrieve2011]

[9] Deductive reasoning. http://en.wikipedia.org/wiki/Deductive_reasoning Wikipedia [retrieve2011]

[10] Wikipedia: http://en.wikipedia.org/wiki/Fermat's-Lasr-Theorem

[11] Tom Davis. Mathematical Induction October 25, 2000

[12] BoZhang. Intertheoretic Reduction andInduction, 2010.

[13] Molnár, G., Greiff, S., & Csapó, B. (2013). Inductive reasoning, domain specific and complex problem solving: Relations and development. *Thinking Skills and Creativity*, 9, 35–45.

[14] Mike Winkler, Uber die Lösberkeit der Diophantischen Gleichung x^n+y^n=z^n April 2004

**Mohamed.AZZEDINE** **October 15, 2021**

azzedine.hamed@gmail.com Tel: +33 6 42 01 86 60 and Tel: +216 52 482 428