Algebraic number theory - Fermat last theorem an elementary proof

Nasr-allah Hitar

January 2023

Abstract

in this paper we will provide a simple proof the Fermat conjecture using a very elementary proof where that (z,p)=1 .

1 introduction

let x,y,z three positive integers and p is an odd prime and (p,z) = 1, suppose that

$$x^p + y^p = z^p \tag{1}$$

Lemma 1 (Fermat little theorem)**.** $(\forall p \in \mathbb{P}) : \forall n \in \mathbb{N} : n^p \equiv n[p]$

Proof. we know that $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ field if and only if p is a prime ; suppose that p is a prime so $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field ; $\therefore$ $(\mathbb{Z}/p\mathbb{Z}-\{0\}, \cdot)$is an abelian group , such that $card(\mathbb{Z}/p\mathbb{Z}-\{0\})$ = p-1 therefore $(\forall a \in \mathbb{Z}/p\mathbb{Z}-\{0\})$ $a^{p-1} = 1$ that give us the lemma. $\square$

Lemma 2. *(gauss theorem corollary)*$(\forall p \in \mathbb{P})(\forall k \in \mathbb{N}) : 0 < k < p : p|\mathrm{C}_p^k$

2 The demonstration principle

Proof. We have that(using **lemma 1**)
$x^p + y^p + z^p \equiv x + y + z[p]$
$\implies 2z^p \equiv x + y + z[p]$ then $2^p z^{p^2} \equiv (x + y + z)^p[p]$
$\therefore$

$$2^p z \equiv \sum_{k=0}^{p} \mathrm{C}_p^k (x + y)^{p-k} z^k [p]$$

as a consequence of **lemma 2**, we have that :
$2^p z \equiv (x + y)^p + z^p \Leftrightarrow 2^p z \equiv (x + y)^p + z$
$\Leftrightarrow z(2^p - 1) \equiv \sum_{k=0}^{p} \mathrm{C}_p^k x^{p-k} y^k [p]$
again using **lemma 2** : we will find that
$z(2^p - 1) \equiv x^p + y^p[p]$
$\therefore z(2^p - 1) \equiv z[p]$
using gauss theorem
$\because$ (z,p) = 1 we could subtract z , therefore :
$2^p \equiv 1[p]$, and while that $p > 2$ we have (p,2) = 1 so using lemma 1 : we will have that : $2^p \equiv 2^{p-1}[p]$ therefore : p = 1
hence! contradiction.
the equation (1) Have no solution .QED. □

Corollary 2.1. *$\forall x, y, z \in \mathbb{Z}_*^3 : \forall n \in \mathbb{N}; n > 3$ and (n,z)=1 the equation (1) have no solution.*

Proof. suppose that there exist an integer $n > 3$ satisfy

$$x^n + y^n = z^n \tag{2}$$

for non-null integers x, y, z
case 1if n is a prime , that's impossible because we proved that (1) have no solution ; **case 2**
if n is not a prime , $\exists p \in \mathbb{P} : p|n \implies (p, q) \in \mathbb{P} \cdot \mathbb{Z}$:

$n = pq \implies (x^q)^p + (y^q)^p = (z^q)^p \therefore$ (1) have a solution; absurd. $\square$

3 References

[1]-Ore, Oystein (1988) [1948], Number Theory and Its History, Dover, ISBN 978-0-486-65620-5.