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.

1 introduction

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

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

Theorem 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. □

2 The demonstration principle

Theorem 2. *the equation*

$$x^{p-1} + y^{p-1} = z^{p-1} \tag{2}$$

has no solution for all prime $p > 3$

Proof. (we supposed that $(xyz, p) = 1$) using $[thm1]$ we get : $x^{p-1} + y^{p-1} + z^{p-1} \equiv 3(modp)$
$\therefore 2(z^{p-1} - 1) \equiv 1(modp) \because (2)$
$\therefore 0 \equiv 1(modp) \because z^{p-1} \equiv 1(modp)$
so that give us the theorem. □

Theorem 3. *(dirichlet theorem) If q and l are relatively prime positive integers, then there are infinitely many primes of the form $l + kq$ with $k \in \mathbb{Z}$*

Proof. <<**See the paper of Zeta relation of primes**>>. □

Corollary 3.1. *Let n be a positive integer with p_n is the nth prime, then there are infinitely many primes of the form $p_1p_2...p_nk + 1$*

Proof. let $q = p_1p_2...p_nk + 1$ and $l = 1$ using [Thm3] that give us the corollary. □

Corollary 3.2. *let $D(n)$ the set of n divisors.*
$\mathbb{P} \subseteq \bigcup_{p\in\mathbb{P}} D(p-1)$

Proof. let's suppose that : $\exists q \in \mathbb{P}\ \forall p \in \mathbb{P}\ q \not| p - 1$
using [Cor3.1] there exist infinite prime of the form $p = (\prod_{i=1}^{q} i)k + 1$ and we have that $q|p - 1$ absurd!. that's give us the corollary. □

Theorem 4. $\forall n \in \mathbb{N}$:$n > 2$ *if the equation*

$$(E_n) : x^n + y^n = z^n \tag{3}$$

has no solution for all integers then all multiples and divisors m , d of n , $(E_m), (E_d)$ have no solution.

Proof. let n a positive integer > 3 , with (E_n) has no solution , suppose there exist a multiple m of n such that , (E_m) has a certain solution we have $\exists q \in \mathbb{N}^*$ $n = qd, m = nq'$ $(E_{dq}, E_{nq'})$ $\therefore$ $(x^q)^n + (y^q)^n = (z^q)^n$
$(x^{q\prime})^d + (y^{q\prime})^d = (z^{q\prime})^d$ have a solution $\therefore$ $(E_n), (E_m)$ have a solution. absurd.that give us the theorem. □

Corollary 4.1. *if the equation (E_p) have no solution for all prime p then the equation (E_n) have no solution for all positive $n > 3$.*

Proof. as we proved in [Thm4] , while we have that for all prime p (E_p) has no solution then for all multiple n of p (E_n) has no solution.($\because \bigcup_{i \in M_p} i = \mathbb{N}$) that's give us the corollary. □

Corollary 4.2. *the equation (1) has no solution with $(xyz, p) = 1$.*

Proof. as corollary of [Cor3.2] and [Thm4] we find that no solution for $(E_p)$for all p prime. □

Corollary 4.3. *if n is a positive integer $n > 3$ and a prime p $p|n$ such that $(xyz, p) = 1$ the equation (E_n) has no solution.*

Proof. that's a corollary of [Thm4]. □

3 references

[1]-Anthony Varilly : Dirichlet's Theorem on Arithmetic Progressions , Harvard University, Cambridge, MA 02138.