Algebraic Number theory : Fermat last theorem

Nasr-allah Hitar

October 2022

1 Introduction :

In number theory, Fermat's Last Theorem (sometimes called Fermat's conjecture, especially in older texts) states that no three positive integers a, b, and c satisfy the equation

$$a^n + b^n = c^n \tag{1}$$

for any integer value of n greater than 2. The cases n = 1 and n = 2 have been known since antiquity to have infinitely many solutions , The proposition was first stated as a theorem by Pierre de Fermat around 1637 in the margin of a copy of Arithmetica. After 358 years of effort by mathematicians, the first successful proof was released in 1994 by Andrew Wiles and formally published in 1995(using Taniyama Shimura conjecture).

2 abc conjecture and applications :

Theorem 1. ***Theorem :(Fermat Last Theorem)*** *No three positive integers a, b, and c satisfy the equation*

$$a^n + b^n = c^n$$

Before proving it We have to talk about abc conjecture

Theorem 2. ***Conjecture : (abc conjecture)*** *For all triples (a, b, c) of coprime positive integers with a + b = c, rad(abc) is at least*

$$c^{1-o(1)}$$

An equivalent formulation is: For every positive real number ϵ, there exists a constant $K\epsilon$
such that for all triples (a, b, c) of coprime positive integers, with a + b = c
We have that

$$: c < k\epsilon(rad(abc))^{1+\epsilon} \tag{2}$$

The conjecture was proved (not officially) by ***Shinichi Mochizuki*** *he proved it using a new* *theory he called* ***inter-universal Teichmüller theory (IUTT)***.

3 abc application to fermat last theorem

let x,y,z three integers such that

$$x^n + y^n = z^n$$

(obviously that x,y,z are co-primes because we could subtract the gcd(x,y,z))
let

$$a = x^n, b = y^n c = z^n$$

so a+b=c and a,b,c are coprimes .
so for every

$$\epsilon > 0 : c < k\epsilon(rad(abc)^{1+\epsilon})$$

$\Rightarrow c < \lim_{\epsilon \to 0} k\epsilon.rad(abc)^{1+\epsilon}$

$$c < k_{0+} rad(abc)$$

$\Rightarrow z^n < (k_{0+} rad((xyz)^n) = k_{0+} rad((xyz)) < k_{0+} xyz)$
(because

$$rad(h^n) = rad(h)$$

and

$$rad(h) \leq h$$

for every integer h)
then

$$z^n < k_{_{0^+}} xyz \Rightarrow z^n < k_{_{0^+}} z^3$$

$(\because x < z$ and $y < z)$

$$n < log_z(k_{0^+}) + 3$$

4 the study of k_{0^+} variant

note : that $k_{0^+} \notin \{\infty\}$ because obviously that : $k_{0^+} < \frac{c}{rad(abc)}$

An elementary result using [(AbdelmajidBenHadjSalem,2019 Thm1]

for any three integers a,b,c such that a coprime with b and a+b=c we have

$$c < rad(abc)^2$$

$$(\forall n \in \mathbb{Z}) : rad(n) \stackrel{\text{def}}{=} \prod_{p|n} p \qquad (3)$$

(such that p is a prime)

let x , y , z , n three positive integers > 0 such that n>2 : and

$$x^n + y^n = z^n$$

we could suppose that x,y are coprimes because it is enough ,
okay let's suppose that x,y are not coprimes so
$\exists p \in \mathbb{P}$:

$$p|x \wedge p|y \to \exists (q,q') \in \mathbb{N}^{*2} : x = p.q \wedge y = p.q'$$

$$\to x^n + y^n = p^n(q^n + q'^n) = z^n \to p|z^n \to p|z \to \exists d \in \mathbb{N} : z = p.d$$
$$\to z^n = p^n d^n \to p^n(q^n + q'^n) = p^n d^n \to q^n + q'^n = d^n$$

and so one until we subtract all coprimes
so after **Thm1 (AbdelmajidBenHadjSalem)** we have
$z^n < rad((xyz)^n)^2 = rad(xyz)^2$
$\to z^n \leq z^6$
$\to n \leq 6 \to n \in \{3,4,5,6\}$
-The case n = 3 was proven by Euler in 1770.
-The case n = 5 was proved by Dirichlet and Legendre around 1825.
-Alternative proofs of the case n = 4 were developed later by Frénicle de Bessy,
-Proofs for n = 6 have been published by Kausler,

5 References

[1]-Abdelmajid Ben Hadj Salem A Note About the ABC Conjecture - A Proof of The Conjecture: $C < rad^2(ABC)$-

2019
-a proof of the abc conjecture after mochizuki (2020) by Go Yamashita.