ALGEBRAIC PROOF IV FERMAT'S LAST THEOREM

James E. Joseph

Department of Mathematics, Howard University, Washington, DC
20059

Abstract:- The special case $z^4 = x^4 + y^4$ is impossible [1]. In view of this fact, it is only necessary to prove, if $x, y, z,$ are relatively prime positive integers, π is an odd prime, $z^\pi \neq x^\pi + y^\pi$ (In this article, the symbol π will represent an odd prime). Also, a new proof is given that $z^4 = x^4 + y^4$ is impossible.

Council for Innovative Research

Peer Review Research Publishing System

Theorem 1 *If* $z^\pi = x^\pi + y^\pi$, *then if* $z \not\equiv 0 \,(mod\, \pi)(y \not\equiv 0 \,(mod\, \pi))[x \not\equiv 0 \,(mod\, \pi)]$,

1. $(x+y)^\pi - z^\pi \equiv 0 \,(mod\, \pi^2), ((z-x)^\pi - y^\pi \equiv 0 \,(mod\, \pi^2)), [(z-y)^\pi - x^\pi \equiv 0 \,(mod\, \pi^2)]$;

2. $(x+y)^\pi - z^\pi \not\equiv 0 \,(mod\, \pi^3), ((z-x)^\pi - y^\pi \not\equiv 0 \,(mod\, \pi^3)), [(z-y)^\pi - x^\pi \not\equiv 0 \,(mod\, \pi^3)]$;

3. $x \equiv 0 \,(mod\, \pi)(y \equiv 0 \,(mod\, \pi))[z \equiv 0 \,(mod\, \pi)]$.

Theorem 1 is arrived at through the following three lemmas.

Lemma 1 *If* $z^\pi = x^\pi + y^\pi$, *then* $x + y - z \equiv 0 \,(mod\, \pi)(z - x - y \equiv 0 \,(mod\, \pi))$.

Proof. It is obvious that

$$(x+y)^\pi - z^\pi \equiv 0 \,(mod\, \pi), (z-y)^\pi - x^\pi \equiv 0 \,(mod\, \pi), (z-x)^\pi - y^\pi \equiv 0 \,(mod\, \pi)$$

$$(x+y)^\pi - z^\pi = (x+y-z+z)^\pi - z^\pi = \sum_0^{\pi-1} C(\pi,k)(x+y-z)^{\pi-k} z^k;$$

$$(1) \quad (x+y)^\pi - z^\pi - (x+y-z)^\pi = \sum_1^{\pi-1} C(\pi,k)(x+y-z)^{\pi-k} z^k.$$

$$(z-x)^\pi - y^\pi = (z-x-y+y)^\pi - y^\pi = \sum_0^{\pi-1} C(\pi,k)(z-x-y)^{\pi-k} y^k;$$

$$(2) \quad (z-x)^\pi - y^\pi - (z-x-y)^\pi = \sum_1^{\pi-1} C(\pi,k)(z-x-y)^{\pi-k} y^k.$$

$$(z-y)^\pi - x^\pi = (z-x-y+x)^\pi - x^\pi = \sum_0^{\pi-1} C(\pi,k)(z-x-y)^{\pi-k} x^k;$$

$$(3) \quad (z-y)^\pi - x^\pi - (z-x-y)^\pi = \sum_1^{\pi-1} C(\pi,k)(z-x-y)^{\pi-k} x^k.$$

Lemma 2 *If* $z^\pi = x^\pi + y^\pi$, *and* $z \not\equiv 0 \,(mod\, \pi)(y \not\equiv 0 \,(mod\, \pi))[x \not\equiv 0 \,(mod\, \pi)]$, *then*
$(x+y)^\pi - z^\pi \equiv 0 \,(mod\, \pi^2)((z-x)^\pi - y^\pi \equiv 0 \,(mod\, \pi^2))[(z-y)^\pi - x^\pi \equiv 0 \,(mod\, \pi^2)]$.

Proof. See proof of Lemma 1.

Lemma 3 *If* $z^\pi = x^\pi + y^\pi$, *and*
$(x+y)^\pi - z^\pi \equiv 0 \,(mod\, \pi^3), ((z-x)^\pi - y^\pi \equiv 0 \,(mod\, \pi^3)), [(z-y)^\pi - x^\pi \equiv 0 \,(mod\, \pi^3)]$, *then*
$z \equiv 0 \,(mod\, \pi); (y \equiv 0 \,(mod\, \pi)); [x \equiv 0 \,(mod\, \pi)]$, *If*
$(x+y)^\pi - z^\pi \equiv 0 \,(mod\, \pi^2)((z-x)^\pi - y^\pi \equiv 0 \,(mod\, \pi^2)), [(z-y)^\pi - x^\pi \equiv 0 \,(mod\, \pi^2)]$, *then*
$z \equiv 0 \,(mod\, \pi); (y \equiv 0 \,(mod\, \pi)); [x \equiv 0 \,(mod\, \pi)]$,

Proof. The first assertion comes from the equations in Lemma 2 and the Unique Factorizaeion Theorem. For the second assertion, if two of the equivalences $x+y \equiv 0 \,(mod\, \pi), z-x \equiv 0 \,(mod\, \pi), z-y \equiv 0 \,(mod\, \pi)$ hold the proof is complete by the equivalence $x+y-z$. Assume $x+y \not\equiv 0 \,(mod\, \pi), z-x \not\equiv 0 \,(mod\, \pi)$, then

$$(x+y)^\pi - z^\pi$$

$$= (x+y)((x+y)^{\pi-1} - z^\pi (x+y)^{-1})$$

$$\equiv 0 \,(mod\, \pi^2)$$

$$= (x+y)((x+y)^{\pi-1} - z^{\pi-1} + z^{\pi-1} - z^{\pi}(x+y)^{-1}) \equiv 0 \ (mod \ \pi^2);$$

$$(x+y)^{\pi-1} - z^{\pi-1} \equiv 0 \ (mod \ \pi);$$

because of the equation

$$(x+y)^{\pi-1} - z^{\pi-1} = (x+y-z)\sum_{0}^{\pi-2}(x+y)^{\pi-1-k} z^k;$$

if

$$(1) \ (x+y)^{\pi-1} - z^{\pi-1} \equiv 0 \ (mod \ \pi^2),$$

Compare this with

$$(2) \ (x+y)^{\pi} - z^{\pi} \equiv 0 \ (mod \ \pi^2),$$

multiplying through (1) by $x+y$ and subtracting (1) from (2) gives

$$z^{\pi-1}(x+y-z)) \equiv 0 \ (mod \ \pi^2);$$

$$z^{\pi-1} \equiv 0 \ (mod \ \pi);$$

thus $z^{\pi-1} \equiv 0 \ (mod \ \pi), z \equiv 0 \ (mod \ \pi).$

If

$$(x+y^{\pi-1} - z^{\pi-1} \not\equiv 0 \ (mod \ \pi^2),$$

then

$$(x+y)\mu\pi \equiv 0 \ (mod \ \pi^2), (\mu,\pi) = 1,$$

so

$$x+y \equiv 0 \ (mod \ \pi),$$

a contradiction.

To show that $y \equiv 0 \ (mod \ \pi).$

$$(z-x)^{\pi} - y^{\pi} = (z-x)^{\pi} - (z-x)y^{\pi}(z-x)^{-1}$$

$$= (z-x)((z-x)^{\pi-1} - y^{\pi-1} + y^{\pi-1} - y^{\pi}(z-x)^{-1}) \equiv 0 \ (mod \ \pi^2);$$

because of the equation

$$(z-x)^{\pi-1} - y^{\pi-1} = (z-x-y)\sum_{0}^{\pi-2}(z-x)^{\pi-1-k} y^k,$$

$$(z-x)^{\pi-1} - y^{\pi-1} \equiv 0 \ (mod \ \pi),;$$

if $((z-x)^{\pi-1} - y^{\pi-1} \equiv 0 \ (mod \ \pi^2),$ this leads to

$$(1) \ (z-x)^{\pi} - y^{\pi} \equiv 0 \ (mod \ \pi^2),$$

$$(2) \ (z-x)^{\pi-1} - y^{\pi-1} \equiv 0 \ (mod \ \pi^2);$$

multiplying through (2) by $z-x$ and subtracting from (1) gives

$$y^{\pi-1}(z-x-y) \equiv 0 \, (mod \, \pi^2);$$

$$y^{\pi-1} \equiv 0 \, (mod \, \pi);$$

thus $y \equiv 0 \, (mod \, \pi)$.

If

$$(z-x)^{\pi-1} - y^{\pi-1} \not\equiv 0 \, (mod \, \pi),$$

then

$$(x+y)\mu\pi \equiv 0 \, (mod \, \pi^2), (\mu, \pi) = 1,$$

so

$$z-x \equiv 0 \, (mod \, \pi),$$

a contradiction.

The paper is finished by producting a new proof of the following theorem.

Theorem 2 *If x, y, z are relatively prime positive integers, then $z^4 \neq x^4 + y^4$.*

Following the proofs above, several equivalences arise:

Proof.

1. $z^2(x+y-z) \equiv 0 \, (mod \, 4);$

2. $y^2(z-x-y) \equiv 0 \, (mod \, 4);$

3. $x+y \equiv 0 \, (mod \, 2);$

4. $z-x \equiv 0 \, (mod \, 2).$

   this leads to $z \equiv 0 \, (mod \, 2), y \equiv 0 \, (mod \, 2)$.

REFERENCES

[1] H. Edwards, Fermat's Last Theorem:A Genetic Introduction to Algebraic Number Theory, Springer-Verlag, New York, (1977).

[2] A. Wiles, Modular ellipic eurves and Fermat's Last Theorem, Ann. Math. 141 (1995), 443-551.

[3] A. Wiles and R. Taylor, Ring-theoretic properties of certain Heche algebras, Ann. Math. 141 (1995), 553-573.