ISSN 2347-1921
Volume 12 Number 1
Journal of Advances in Mathematics

2016 algebraic proof Fermats last theorem (2-18)

James E. Joseph

ABSTRACT

For other theorems named after Pierre de Fermat, see the book by H. Edwards [1]. The 1670 edition of Diophantus' Arithmetica includes Fermat's commentary, particularly his "Last Theorem" (Observatio Domini Petri de Fermat). In number theory, Fermat's Last Theorem (sometimes called Fermat's conjecture, especially in older texts) states that no three positive integers x, y, and z satisfy the equation $z^{\pi} = x^{\pi} + y^{\pi}$ for any integer value of π greater than two. The case $\pi = 2$ was known to have infinitely many solutions. This theorem was first conjectured by Pierre de Fermat in 1637 in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin. The first proof agreed upon as successful was released in 1994 by Andrew Wiles, using cyclic groups (a subject area which was studied at the time of Fermat), and formally published in 1995, after 358 years of effort by mathematicians. The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among the most notable theorems in the history of mathematics It is known that if x, y, z are relatively prime positive integers, $z^4 \neq x^4 + y^4$[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, $z^{\pi} = x^{\pi} + y^{\pi}$, then $x, y, z,$ are each divisible by π. Before and since Wiles papers [2], [3], many papers and books have been written trying to solve this problem in an elegant algebraic way, but none have suceeded. (See [1], and go to a search engine on the computer and search Fermats Last Theorem). In the remainder of this paper, π will represent an odd prime.

Theorem 1 If $x, y, z,$ are positive integers, and $z^{\pi} = x^{\pi} + y^{\pi}$, then $x, y, z,$ are each divisible by π.

Theorem 1 is arrived at by lemmas.

Lemma 1 If $z^{\pi} = x^{\pi} + y^{\pi}$, then

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

Proof.

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

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

the result follows since

$$(x+y)^{\pi} - z^{\pi} \equiv 0 \,(mod\ \pi), \sum_{1}^{\pi-1} C(\pi,k)(x+y-z)^{\pi-k} z^{k} \equiv 0 \,(mod\ \pi^2); x+y-z \equiv 0 \,(mod\ \pi), \pi > 2.$$

Lemma 2 If $x, y, z,$ are relatively prime positive integers, and $z^{\pi} = x^{\pi} + y^{\pi}$, then
$z \equiv 0 \,(mod\ \pi)(y \equiv 0 \,(mod\ \pi));$

Proof. First, $z \equiv 0 \,(mod\ \pi)$. It is clear that $z^{\pi} - (x^{\pi} + y^{\pi}) \equiv 0 \,(mod\ \pi^{\pi});$ so $z \equiv 0 \,(mod\ \pi);$

$y \equiv 0 \,(mod\ \pi)$. Using $z \equiv 0 \,(mod\ \pi)$, it follows that

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

From $z \equiv 0 \,(mod\ \pi), x^{\pi} + y^{\pi} = (x+y)\sum_{0}^{\pi-1} z^{\pi-1-k} y^{k} \equiv 0 \,(mod\ \pi^{\pi})$. So
$\sum_{0}^{\pi-1} z^{\pi-1-k} y^{k} \equiv 0 \,(mod\ \pi^{\pi-1}), y^{\pi-1} \equiv 0 \,(mod\ \pi)$. and $y \equiv 0 \,(mod\ \pi))$

Fermat's Last Theorem If $x, y, z,$ are relatively prime positive integers, then $z^{\pi} \neq x^{\pi} + y^{\pi}$.

Proof. From Lemma 1. $x+y-z \equiv 0\,(mod\ \pi), z \equiv 0\,(mod\ \pi), y \equiv 0\,(mod\ \pi)$ by Lemma 1. So $x, y, z,$ are not relatively prime.

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 ofcertain Heche algebras, Ann. Math. 141 (1995), 553-573.