Journal of Progressive Research in Mathematics(JPRM)
ISSN: 2395-0218

SCITECH
RESEARCH ORGANISATION|

Volume 4, Issue 4
Published online: August 08, 2015|

Journal of Progressive Research in Mathematics
www.scitecresearch.com/journals

An algebraic proof of Fermat's last theorem

James E. Joseph
Department of Mathematics
Howard University
Washington, DC 20059.

Abstract:

In 1995, A, Wiles announced, using cyclic groups, a proof of Fermat's Last Theorem, which is stated as follows: If π is an odd prime and x, y, z are relatively prime positive integers, then $z^{\pi} \neq x^{\pi} + y^{\pi}$. In this note, a proof of this theorem is offered, using elementary Algebra. It is proved that if π is an odd prime and x, y, z are positive inyegera satisfying $z^{\pi} = x^{\pi} + y^{\pi}$, then $x, y,$ and z are each divisible by π.

Key words and phrases: Fermat.

2010 Mathematics Subject Classification: Primary 11Yxx.

The special case $z^4 = x^4 + y^4$ is impossible for rekatively prime integers x, y, z [1]; it is only necessary to show that if $x, y, z,$ are relatively prime positive integers, π is an odd prime, $z^{\pi} \neq x^{\pi} + y^{\pi}$. If x and π are positive integers, the notation $x \equiv 0\,(mod\ \pi)$ will mean x is divisible by π. Let $C(\pi.k)$ represent the k^{th} coefficient of the binomial expansion of $(x+y)^{\pi}$; if π is prime, then $C(\pi, k) \equiv 0\,(mod\ \pi)$ for every $1 < k < \pi$.

Theorem 1. *If x, y, z are positive integers, π an odd prime and $x^{\pi} + y^{\pi} = z^{\pi}$, then $x \equiv 0\,(mod\ \pi)$, $y \equiv 0\,(mod\ \pi), z \equiv 0\,(mod\ \pi)$.*

Theorem 1 is arrived at as a result of two Lemmas.

Lemma 1. *If x, y, z are positive integers, π an odd prime, and $z^{\pi} = x^{\pi} + y^{\pi}$, then*

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

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

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

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

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

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

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

(8) $x+y-z \neq 0.$

Proof. Using the equation $z^{\pi}=x^{\pi}+y^{\pi}$, statemente (1), (2), and (3) are obvious; (4), (5), (6), and (7) come from the equations

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

$$(eq.2)\ \ (z-y)^{\pi}-x^{\pi}-(z-x-y)^{\pi}=\sum_{1}^{\pi-1}C(\pi,k)(z-x-y)^{\pi-k}x^{k};$$

$$(eq.3)\ \ (z-x)^{\pi}-y^{\pi}-(z-x-y)^{\pi}=\sum_{1}^{\pi-1}C(\pi,k)(z-x-y)^{\pi-k}y^{k};$$

and the fundamental theorem of Arithmetic; (8) is obvious. leading to $xy=0$.

Lemma 2. *If* π *is an odd prime and* x,y,z *are positive integers such that* $z^{\pi}=x^{\pi}+y^{\pi}$, *then*

(1) $xy \equiv 0\ (mod\ \pi);$

(2) $yz \equiv 0\ (mod\ \pi);$

(3) $xz \equiv 0\ (mod\ \pi).$

Proof.

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

there is a k with $C(\pi,k)x^{\pi-k}y^{k}\equiv 0\ (mod\ \pi^{2});$ order $C(\pi,k)x^{\pi-k}y^{k}$ by inclusion and there exists k such that $C(\pi,k)x^{\pi-k}y^{k}\equiv 0\ (mod\ \pi^{2});$

$$(F1)\ \ x^{\pi-k}y^{k}\equiv 0\ (mod\ \pi);$$

multiplying by $x^{k}y^{\pi-k}$ gives $(xy)^{\pi}\equiv 0\ (mod\ \pi)$ which implies

$$(F1^{*})\qquad xy\equiv 0\ (mod\ \pi).$$

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

there is a k with $C(\pi,k)y^{\pi-k}z^{k}\equiv 0\ (mod\ \pi^{2});$ order $C(\pi,k)y^{\pi-k}z^{k}$ by inclusion and there exists k such that $C(\pi,k)y^{\pi-k}z^{k}\equiv 0\ (mod\ \pi^{2});$

$$(F2)\ \ y^{\pi-k}z^{k}\equiv 0\ (mod\ \pi);$$

multiplying by $y^{k}z^{\pi-k}$ gives $(yz)^{\pi}\equiv 0\ (mod\ \pi)$ which implies

$$(F2^{*})\qquad yz\equiv 0\ (mod\ \pi).$$

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

there is a k with $C(\pi,k)x^{\pi-k}z^{k}\equiv 0\ (mod\ \pi^{2});$ order $C(\pi,k)x^{\pi-k}z^{k}$ by inclusion and there exists k such that $C(\pi,k)x^{\pi-k}z^{k}\equiv 0\ (mod\ \pi^{2});$

$$(F3)\; x^{\pi-k}z^k \equiv 0\,(mod\;\pi);$$

multiplying by $x^k z^{\pi-k}$ gives $(xz)^\pi \equiv 0\,(mod\;\pi)$ which implies

$$(F3^*)\quad xz \equiv 0\,(mod\;\pi).$$

The last three equivalences $(F1^*),(F2^*),(F3^*),$ along with $x+y-z\equiv 0\,(mod\;\pi)$ complete the proof.

Fermat's Last Theorem. If π is an odd prime and x,y,z are relatively prime positive integers, then $z^\pi \neq x^\pi + y^\pi$.

Proof. If π is an odd prime. then $z\equiv 0\,(mod\;\pi); y\equiv 0\,(mod\;\pi) x\equiv 0\,(mod\;\pi).$

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.******Order $C(\pi,k)x^{\pi-k}y^k$ by magnitude and there exists k such that $C(\pi,k)x^{\pi-k}y^k \equiv 0\,(mod\;\pi^2)$ *****Wiles and R. Taylor, Ring-theoretic properties of certain Heche algebras, Ann. Math. 141 (1995), 553-573. *****

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

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

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

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

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

$$z \equiv 0\,(mod\;\pi).$$

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

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

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

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

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

$$x \equiv 0\ (mod\ \pi).$$