R.A.D.Piyadasa & B.B.U.P.Perera
Department of Mathematics, University of Kelaniya

Poster

Integer roots of two polynomial equations and a simple proof of Fermat's last theorem

Fermat's last theorem (FLT),possibly written in 1637,despite its rather simple statement, is very difficult to prove for general exponent n[1]. In fact, formal complete proof of FLT remained illusive until 1995 when Andrew Wiles and Taylor[1],[2] put forward one based on elliptic curves[3]. It is well known that their proof is lengthy and difficult to understand. Main objective of this paper is to provide a simpler and shorter proof for FLT. It is shown that FLT can be proved by showing that two polynomial equations have no integer roots when the independent variable satisfies certain conditions.

Theorem: The polynomial equations in x

$$x^p - 2.p^m uhdx - (h^p + p^{pm-1}u^p) = 0$$

$$x^p - 2uhdp^m x - (h^p + u^p) = 0$$

where u, h, p, d are integers co-prime to one another , p is an odd prime and $m \geq 2$, have no integer roots co-prime to h for any integer values of it when u, h are both odd or of opposite parity[4],[5].

Lemma

If $F(a,b) = a^p - b^p \equiv 0(\bmod p^m)$ and $(a,p) = (b,p) = 1$, then $a - b \equiv 0(\bmod p^{m-1})$ and $m \geq 2$

Proof of the theorem: We first consider the equation

$$x^p - 2.p^m uhdx - (h^p + p^{pm-1}u^p) = 0$$

The integer roots of this equation are the integer factors of $h^p + p^{pm-1}u^p$ and let us assume that it has an integer root. This integer root obviously must be co-prime to u, h, p since they are co-prime. If an integer satisfies the equation , then

$$(g^p - h^p) - 2.p^m uhd - p^{pm-1}u^p) = 0$$

and $g - h \equiv 0(\bmod p^{m-1})$. Therefore, we can write $g = h + p^{m=1} j$, where the integer j is co-prime to d, h, p .Now, our equation can be written as

$$(h + p^{m-1} j)[(h + p^{m-1} j)^{p-1} - 2uhdp^m] = h^p + p^{pm-1}u^p$$

and we use the remainder theorem to check weather the linear factor $h + p^{m-1} j$ in h a factor of the polynomial $h^p + p^{pm-1}u^p$ in h. If so,

$$-p^{pm-p} j^p + p^{pm-1}u^p = 0$$

This is impossible since $(j, p) = 1$, and we conclude that (1) has no integer roots we need.

If g satisfies the equation

$$g^p - 2uhdp^m g - (h^p + u^p) = 0$$

and g must be a factor of $h^p + u^p$. We also assume that h, u are both odd or of opposite parity which is relevant to Fermat's last theorem. First of all, we will show that $g \neq h + u$ using the relation

$$h^p + u^p \equiv (h+u)^p + \sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i}.(-1)^i.{}^{p-1-i}C_{i-1} u^i h^i (h+u)^{p-2i}$$

Our equation takes the form

$$g^{p}-(h+u)^{p}-2ughdp^{m}-\sum_{i=1}^{\frac{p-1}{2}}\frac{p}{i}.(-1)^{i}.{}^{p-1-i}C_{i-1}.u^{i}h^{i}(h+u)^{p-2i}=0$$

If $g=h+u\neq 0$, then we must have

$$-2dp^{m}-[p.(h+u)^{p-3}+\frac{p}{2}\;{}^{p-3}C_{1}uh(h+u)^{p-5}-\cdots+p(-1)^{\frac{p-1}{2}}u^{\frac{p-3}{2}}h^{\frac{p-3}{2}}]=0$$

If both u and h are odd, or , of opposite parity ,then the term

$$-[p.(h+u)^{p-3}+\frac{p}{2}\;{}^{p-3}C_{1}uh(h+u)^{p-4}-\cdots+p(-1)^{\frac{p-1}{2}}u^{\frac{p-3}{2}}h^{\frac{p-3}{2}}]$$

is odd since $p(\geq 3)$ is an odd prime and therefore the equation

$$-2dp^{m}-[p.(h+u)^{p-3}+\frac{p}{2}\;{}^{p-3}C_{1}uh(h+u)^{p-5}-\cdots+p(-1)^{\frac{p-1}{2}}u^{\frac{p-3}{2}}h^{\frac{p-3}{2}}]=0$$

will never be satisfied since $2dp^{m}$ is even. Hence, $g\neq h+u$. From the equation

$$g^{p}-(h+u)^{p}-2ughdp^{m}-\sum_{i=1}^{\frac{p-1}{2}}\frac{p}{i}.(-1)^{i}.{}^{p-1-i}C_{i-1}.u^{i}h^{i}(h+u)^{p-2i}=0$$

we conclude that $g-(h+u)\equiv 0(\bmod p)$, which follows from the lemma Therefore , we can write $g=h+(u+p^{k}j)$, where $k\geq 1$, $j\neq 0$ and $((u+p^{k}j),h)=1$ is since $(g,h)=1$. Since $g=h+(u+p^{k}j)$ is an integer root of the equation we can write

$$h^{p}+u^{p}=[h+(u+p^{k}j)][(h+u+p^{k}j)^{p-1}-2uhdp^{m}]$$

As before , using the remainder theorem, we get

$$(u+p^{k}j)^{p}-u^{p}=0$$

But this equation will never be satisfied since $j\neq 0$.

References

(1) P.Ribenboim, Fermat’s last theorem for amateurs, Springer-Verlag, New York, 1991.

(2) H.M. Edwards, Fermat’s last theorem, A Genetic Introduction to Algebraic Number Theory, Springer -Verlag, 1977.

(3) Andrew Wiles, Modular elliptic curves and Fermat’s last theorem, Annals of Mathematics, 141(3),(1995),443-551

(4)R.A.D.Piyadasa, Simple analytical proof of Fermat’s last theorem for $n=7$, CMNSEM,Vol.1,No.7.October 2010,p.163-168

(5)R.A.D.Piyadasa, Simple short analytical proof of Fermat’s last theorem , CMNSEM,Vol.2,No.3.March 2011,p.57-63