Title: Fermat's Last Theorem

Author: Barry Foster

Abstract: Recall the theorem states that the equation $a^n + b^n = c^n$ cannot exist if all quantities are positive integers and n>2. Fermat maintained he had a short proof but it has never been found, nor has a short proof been supplied by anyone since. This attempt uses simple mathematics and methods reminiscent of those taught in English grammar schools in the 1950's.

Fermat's Last Theorem
"Hanson Boys' G. S. Proof"

Statement of the Theorem

Fermat's Last Theorem **(FLT)** states that positive integers {a,b,c} cannot be found satisfying the equation:

$$a^n + b^n = c^n \qquad \textbf{(T)}$$

for any integer value of n greater than 2.

Proof

Assume n is prime.

{

If n is not prime, say $n=p_1p_2....p_r$, where the p_i are primes, not necessarily all different, we may rename p_1 to n, and {a, b, c} then become integers raised to the power ($p_2...p_r$).

To clarify, the equation:

$$u^{p1p2....pr}+v^{p1p2....pr}=w^{p1p2....pr} \qquad \{u,v,w \text{ positive integers; } u<v<w\}$$

becomes $u^{n(p2....pr)}+v^{n(p2....pr)}=w^{n(p2....pr)}$

i.e. $a^n + b^n=c^n$ *where* $a=u^{(p2....pr)}$ $b=v^{(p2....pr)}$, $c=w^{(p2....pr)}$

}

Assume that all common factors have been cancelled, noting that all or none of {a,b,c} have a common factor. **(A)**

Assume the theorem is false and n is an integer >2 such that positive integers {a,b,c} **do** exist satisfying the equation:

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

Assume a<b, thus a<b<c.

Let $a + h = b + i = c$ {h, i integers, h>i}

Then $a^n + b^n = (a + h)^n = (b + i)^n = c^n$

We can rewrite **(T)** in 2 different ways:

(I) Using the Binomial Theorem

$$a^n = (b + i)^n - b^n = nb^{n-1}i + n(n-1)/(2!)b^{n-2}i^2 +......+ i^n$$

$$b^n = (a + h)^n - a^n = na^{n-1}h + n(n-1)/(2!)a^{n-2}h^2 +......+ h^n$$

(II) By factoring

$$a^n = (c - b)(c^{n-1} + c^{n-2} b + ... + b^{n-1})$$

$$= i(c^{n-1} + c^{n-2} b + ... + b^{n-1})$$

$$b^n = (c - a)(c^{n-1} + c^{n-2} a + ... + a^{n-1})$$

$$= h(c^{n-1} + c^{n-2} a + ... + a^{n-1})$$

let $a = Gy$ {G,y integers>0, G = product of primes **not in** i,
y = product of primes **in** i}
and $b = Fx$ {F,x integers>0, F = product of primes **not in** h,
x = product of primes **in** h}

then x>y (∵ h>i) and {x,y co-prime ∵ of (A)}

The equations in **(I)** may now be written:

$$(Gy)^n = i(nb^{n-1} + n(n-1)/(2!)b^{n-2}i + \ldots\ldots + i^{n-1}) \qquad \mathbf{\{i <= y^n\}}$$
$$(Fx)^n = h(na^{n-1} + n(n-1)/(2!)a^{n-2}h + \ldots\ldots + h^{n-1}) \qquad \mathbf{\{h<= x^n\}}$$

let $i= y^p$ {0<p<=n}
dividing through by y^p gives:

$$G^n y^{n-p} = nb^{n-1} + n(n-1)/(2!)b^{n-2}i + \ldots\ldots + i^{n-1}$$

Since y now occurs in every term except nbn-1 this requires:

p=n or, p=n-1 and n=y, (y cannot be in b^{n-1} ∵ of **(A)**)

If p=n-1 and n=y n is a factor of a and **(T)** may now be written:

$$(An^q)^n + b^n = c^n$$ {1<=q; q integer, A=product of all primes in a other than n}

∴ $n^q = (c^n – b^n)^{1/n}/A$ and n is not prime.

Thus $\mathbf{i = y^n}$ and similarly $\mathbf{x = h^n}$**.**

(II) can now be written

$$(Gy)^n = y^n(c^{n-1} + c^{n-2}b + \ldots.\ b^{n-1})$$
$$G^n = (c^{n-1} + c^{n-2}b + \ldots.\ b^{n-1})$$
$$(Fx)^n = x^n(c^{n-1} + c^{n-2}a + \ldots.\ a^{n-1})$$
$$F^n = (c^{n-1} + c^{n-2}a + \ldots.\ a^{n-1})$$

∴ **G>F {but Fx>Gy ∵ Fx=b and Gy=a; a<b}** **(B)**

since $a + h = b + i = c$
$Gy + x^n = Fx + y^n = c$
∴ $Fx - Gy = x^n - y^n$
$= (x-y)(x^{n-1} + x^{n-2}y \ldots.\ xy^{n-2} + y^{n-1})$
$= (x-y) R$ $\{R = (x^{n-1} + x^{n-2}y \ldots\ xy^{n-2} + y^{n-1})$ **(C)**

from **(C),** writing F + w for G {w integer>0}
$Fx – (F + w)y = R(x-y)$
$F(x – y) = R(x-y) + wy$
∴ **F>R**
and **G>F>R** from **(B)**

let	$F = (R + u), G = (R + v)$ {u,v integers, u>v>0}
$\therefore$	$(R + u)x - (R + v)y = R(x-y)$
giving	$ux = vy$

This is a contradiction $\because$ $u>v$ and $x>y$.

Therefore the conclusion must be that Fermat’s Last Theorem is true.