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 the 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' Grammar School Proof"

Statement of the Theorem

Fermat's Last Theorem, (FLT), states that positive integers {a,b,c,n; n>2} cannot be found satisfying the equation:

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

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* $a = u^{(p2...pr)}, b = v^{(p2...pr)}, c = w^{(p2pr)}$

}

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

Assume the theorem is false and n is an integer >2 such that positive integers {a,b,c} exist satisfying **(T)**.

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

let $a+h = b+j = c$ {h, j positive integers; h>j} **(1)**

We can now rearrange **(T)** and expand a^n and b^n in 2 different ways.

(i) Using the Binomial Theorem

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

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

(ii) By factoring

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

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

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

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

Let $a=Ay$ {A,y integers>0; A = product of primes **not in** j, y = product of primes **in** j}

and $b=Bx$ {B,x integers>0; B = product of primes **not in** h, x = product of primes **in** h}

thus $x>y$ {h>j; x,y are co-prime ∵ of **(F)**}

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

$(Ay)^n = j(nb^{n-1}+n(n-1)/(2!)b^{n-2}j + ... + j^{n-1})$ $\{j <= y^n\}$ **(i.1)**
$(Bx)^n = h(na^{n-1}+n(n-1)/(2!)a^{n-2}h + ... + h^{n-1})$ $\{h <= x^n\}$ **(i.2)**

(i.1) divided by j gives:

$A^n = nb^{n-1} + n(n-1)/(2!)b^{n-2}j + ... + j^{n-1}$ $\{\text{if } j=y^n\}$ **(1.1a) or**
$A^nY = nb^{n-1} + n(n-1)/(2!)b^{n-2}j + ... + j^{n-1}$ $\{\text{if } j<y^n\}$ **(1.1b)**

Y is the product of primes remaining from y^n after dividing and necessarily contains n since n is in every term on the RHS.

Case 1: Assume (1.1a) is true.

Arguing similarly for **(i.2)** gives $j=y^n$, $h=x^n$

from **(1)** $Ay + x^n = Bx + y^n = c$ **(2)**

and since $(a + b)^n > a^n + b^n\ (=c^n)$
$(a + b) > c$

∴ $Ay + Bx > Ay + x^n$
$Ay + Bx > Bx + y^n$

thus $Bx > x^n;\ Ay > y^n$

from **(2)** $Bx – Ay = x^n - y^n = k$ {k; positive integer} **(2.1)**
$= R(x - y)$ $\{R = x^{n-1}+ x^{n-2}y + ... + y^{n-1}\}$ **(2.2)**
$= Xx - Yy$ $\{X = x^{n-1}, Y = y^{n-1}\}$ **(2.3)**

from **(ii)** $A>B$ $\{(Ay)^n = y^n (c^{n-1}+c^{n-2} b+...+b^{n-1});\ A^n = c^{n-1}+...+b^{n-1}$
$(Bx)^n = x^n(c^{n-1}+c^{n-2} a+...+a^{n-1});\ B^n = c^{n-1}+...+a^{n-1})\}$

from **(2.2)** $B>R$ $\{Bx – Ay = B(x – y) – (A – B)y = R(x – y)\}$

∴ $Bx>Ay>A>B>R>X>Y$

let $A = R + u;\ B = R + v$ {u, v positive integers, u<v}
$(R + v)x – (R + u)y = R(x – y)$ {from **2.1** and **2.2**}
$vx = uy$

∴ $u=x,\ v=y$ **(3)** {not u=Py, v=Px, P positive integer;
∵ x, y coprime}

(2.1) – (2.3) are supposedly consistent simultaneous linear equations. This requires **(2.1)** to be a linear combination of **(2.2)** and **(2.3)**

∴ $B = pR + qX$ {p, q; real}
$A = pR + qY$
$k = pk + qk$

thus $p + q = 1$

∴ $A - B = pR + qY - (pR + qX)$
$= q(Y - X)$ $\{q<0 ; A>B, X>Y\}$

since $R + v = B$
$R + v = pR + qX$
$v = (p - 1)R + qX$
$v = q(X - R)$
but from **(3)** $v = y$

This is a contradiction and proves FLT.

Case 2: Assume (1.1b) is true.

Note that n cannot be a factor of both Ay and Bx (∵ of **(F)**). Furthermore, because **(1.1b)** contains factors in Y that are in every j on the RHS, those factors cannot be in b of the first term (∵ of (F)).

Therefore Y, y, and j must have the forms:
$Y= n^{nr}$, $y=tn^{r}$, $j=t^{n}n^{nr-1}$ $\{r$ integer>0, $t=$product of primes in y other than n$\}$

∴ **(2)** becomes:

$$Aw + x^{n} = Bx + (w/n^{(1/n)})^{n} = c \quad \{w=tn^{r}\}$$

and we proceed as for Case 1 to the same contradiction.