A proof of Fermat's Last Theorem

BY RAMASWAMY KRISHNAN
B7/203 VIJAY PARK THANE INDIA-400615
email: ramasa421@gmail.com

SYNOPSIS:
This proof is based on an assumption that the value of an infinite series cannot be obtained from a finite number of terms of the series. For all possible factors of \((x+y-z)\), three infinite series can be developed, two convergent and one divergent. In all the three cases the value of the infinite series can be obtained by considering only a finite number of terms. This gives the value for \((x+y-z) = p_1^{\alpha} p_2 p_3\), thus proving Fermat's last theorem.

Proof:

If \(x^p + y^p = z^p\) where 'p' is a prime number, it is well known that integers \(p_1, p_2, p_3, q_1, q_2, q_3\) and \(\alpha\) exist such that \(x = p_1 q_1, y = p_2 q_2, z = p_3 q_3\), and \(z-y = p_1^{p_1^\alpha} p_3\), \(z-x = p_2^{p_1^\alpha} p_3\), \(x+y = p_3^{p_1^\alpha} q_3\) if \(p\) is prime to \(x, y, z\) and if \(p\) is a divisor of one of them say \(z\) then \(z = p_1^{\alpha} p_3\).

\[
x+y-z \equiv 0 \pmod{(p_1 p_2 p_3)}
\]

is obvious. It is easy to prove that \(x+y-z \equiv 0 \pmod{p_1^\alpha p_2 p_3}\) and \(\alpha \ge 3\). Further, \(\text{HCF of} (x+y)(x+y)(x+y) = \frac{xy + y(x+y)(x+y) + x+y}{2}\) can have a common factor say \(p_4\). Therefore, it can be concluded that \(x+y-z = p_1^{\alpha} p_2 p_3 p_4^{l}\).
where \( l = 1 \) or \( 2 \). Let us assume that 'p' is prime to \( x, y, z \). \( z \equiv x + y \mod (p^\alpha) \) ——-So we can take \( z = (x + y) + k_1 p^\alpha \); \( \therefore z^p \equiv (x + y)^p \mod (p^{2\alpha + 1}) \)  ——— (1)

From (1) \( k_1 \equiv \frac{1}{p} \cdot \frac{x^p + y^p - (x + y)^p}{(x + y)^{p-1}} \mod (p^{2\alpha + 1}) \) ——— (2)

This can be continued further \( k_2 \equiv p^{2\alpha}, k_3 \equiv p^{3\alpha}, k_4 \equiv p^{4\alpha}, \ldots, k_r \equiv p^{r\alpha}, \ldots \) up to \( \infty \)

Let \( Q = \frac{x^p + y^p - (x + y)^p}{p(x + y)} \equiv 0 \mod (p^\alpha) \) and \( \not\equiv 0 \mod (p^{\alpha + 1}) \)

because \( x + y - z \equiv 0 \mod (p^\alpha) \) ——— (3)

\( \frac{1}{p} \cdot \frac{C_r}{r!} = \frac{1}{r!} (1 - p)(1 - 2p)(1 - 3p) \ldots (1 - rp + 1) \) ——— (4)

then \( k_r \equiv \frac{1}{p} \cdot \frac{C_r}{r!} Q^r (x + y) \mod (p^{\alpha + 1}) \) where \( (r + 1)! \equiv 0 \mod (p^\gamma) \)

\( \beta + \alpha = \frac{(r + 1)\alpha}{\gamma} \) ——— (5)

\( \therefore \)

\( z \equiv (x + y) + (x + y) \sum_{1}^{r} \frac{1}{p} \cdot \frac{C_r}{r!} Q^r \mod (p^{\beta + \alpha}) \) ——— (6)

Basically eqn (6) is the expansion of \( \frac{z}{x + y} = \left\{1 + \frac{x^p + y^p - (x + y)^p}{(x + y)^{p-1}}\right\}^{\frac{1}{p}} \)

Now if \( z \mod (p^\alpha) \equiv \beta + \alpha \mod (p^\alpha) \)

\( \sum_{1}^{r} \frac{r}{p} \cdot \frac{C_r}{r!} \mod (Q^r) \equiv R \mod (p^{\alpha + 1}) \) ——— (6)

Basically eqn (6) is the expansion of \( \frac{z}{x + y} \) where \( x, y \) and \( z \) are not divisible by \( p \)

For a given \( x, y, z \) the value of an infinite series can be obtained by using a finite number of terms. As this is not possible either \( z \) is irrational or 'p' is a divisor of \( x \) or \( y \) or \( z \).
series quadratic can be developed using $z$ and $x$ and $z$ and $y$ which are given by
\[
\frac{x}{z-y} = \left\{ 1 + \frac{z^p - y^p - (z-y)^p}{(z-y)^p} \right\}^{\frac{1}{p}}
\]
\[
\frac{y}{z-x} = \left\{ 1 + \frac{z^p - x^p - (z-x)^p}{(z-x)^p} \right\}^{\frac{1}{p}}
\]
If $y < x$ then $2x > z$ or $x > (z-x)$
\[
\frac{z^p - x^p - (z-x)^p}{(z-x)^p} = \left(\frac{z}{z-x}\right)^{p-1} + \left(\frac{z}{z-x}\right)^{p-2}\left(\frac{x}{z-x}\right) + \cdots + \left(\frac{x}{z-x}\right)^{p-1}
\]
\[-1 > 1\]
\[
\therefore the terms in the series developed for $y$ will tend to $+\infty$ or $-\infty$.
\[
\therefore given z and x with $2x > z$ $y$ has to be irrational or $p$ is a divisor of $x$, $y$, or $z$.
\[
x, y, z, p_4, p_5$ are prime to each other.
\[
\therefore if $q^r$ is a factor of either $p_4$ or $p_5$ and $x+y-z$ then what is applicable to $p$ is also applicable to $q$.
\[
\therefore r = 0$ or $p_4 = 1$ and $p_5 = 1$
\[
hence (x+y-z) = p^{\alpha}p_1p_2p_3$.
\[
\therefore p^{p\alpha - 1}p_3^p - p_1^p - p_2^p = 2p^{\alpha}p_1p_2p_3 \quad \text{(8)}
\]
As eqn (8) has no solution Fermat's last theorem stands proved.