AN ELEGANT PROOF OF FERMAT'S LAST THEOREM

John H. W. Sall

currently on leave of absence from
Department of Mathematics and Statistics
Queen's University, Kingston, Canada, K7L 3N6

A historical introduction. The early seventeenth century French mathematician, Pierre de Fermat, announced that he had proved the following result:

for each integer \( n > 2 \), an \( n \)-th power of an integer cannot be the sum of two \( n \)-th powers of integers.

However, no proof was received from Fermat, and no proof was discovered in Fermat's papers after Fermat's death. The result was thus a conjecture until late in the twentieth century. However, it was named Fermat's Last Theorem.

This research article proves Fermat's Last Theorem in an elegant way, which method could have been used by Fermat. Fermat's Last Theorem may already
have been proved by Wiles, whose proof is under intense scrutiny. The proof by Wiles could not have been invented by Fermat and this fact justifies the publication here of a proof which Fermat could have created.

In order that Fermat's Last Theorem be valid for all integer exponents $n > 2$, it clearly must be true for all prime exponents $p > 2$. Indeed, these prime exponents are very important because Fermat's last theorem is true for all integer exponents $n > 2$ if it is true for the exponent $n = 4$ and for all prime exponents $p > 2$. Among Fermat's known writings is a proof for $n = 4$ using the method of infinite descent. Thus it remains to prove Fermat's last theorem for all prime exponents $p > 2$. This will be achieved.

The main result: We state and prove the following.

**Theorem 1.** If $p$ is a prime and $p > 2$
and \( x, y, z \) are integers, not necessarily positive, such that \( x, y, z \) are relatively prime in pairs, then \( x^p + y^p \neq z^p \).

**Proof.** Assume otherwise and obtain a contradiction. Let \( p \) be prime and let \( x, y, z \) be integers, not necessarily all positive but relatively prime in pairs, such that \( x^p + y^p = z^p \).

\[
\begin{align*}
\left( x^p + y^p \right)^2 &= (x+y)(x^{p-1} - xy^{p-2} + y^{p-1}) \\
&= (x+y) \left( x^{p-2} + 2y x^{p-3} + 3y^2 x^{p-4} + \ldots + y^{p-1} \right) \\
&= (x+y) \left( x^{p-2} + y^{p-1} \right)
\end{align*}
\]

Any factor of the gcd of \((x+y)\) and \((x^{p-1} - xy^{p-2} + y^{p-1})\) must also be a factor of \( p y^{p-1} \). If a factor of \( y \) and \((x+y)\) it is a factor of \( x \) also and thus \( x, y \) are not relatively prime if the factor is greater than 1. Any factor greater than 1 must be \( p \), but it cannot be ruled out that 1 is the only common factor. Let \( q \) be a factor of \((x+y)\) and \( q \neq p \). If \( p \) divides \( z \), interchange the role of \( y \) and \( z \), so that now \( p \) does not divide \( z \).
Then, if $\mathcal{Z} = Bq^b$, with $b > 0$ and $b, B$ integers and $q$ does not divide $B$, it follows that integer $k$ exists such that $y = (B - k) = (Bq^b - k)$. Furthermore, $(x + y) \equiv 0 \pmod{q}$, so $x = (Aq^a + k)$, where $a > 0$ and $q, A$ are integers, and $q$ does not divide $A$. Let $k$ be divisible by $q$.

Now look at

$$Bq^b = (Bq^b)^p = x^p + y^p = (Aq^a + k)^p + (Bq^b - k)^p = (Aq^a)^p + \ldots + (1)(Aq^a)k^{p-1} + k^p + (Bq^b)^p - \ldots - (1)(Bq^b)k^{p-1} - k^p$$

In equation (1), assume that $a > b$. Then modulo $q^{b+1}$, equation (1) is

$$(1)(Bq^b)k^{p-1} \equiv 0 \pmod{q^{b+1}} \quad \cdots (2)$$

By choice, $q + p$ and $B$ and $k$ are each not divisible by $q$, congruence (2) is a contradiction. Thus, $a \leq b$.

If $a \leq b$, then modulo $q^{b+1}$, equation (1) is

$$(1)(Aq^a)k^{p-1} \equiv 0 \pmod{q^{b+1}} \quad \cdots (3)$$

By choice, $q + p$ and $q$ does not divide $A$ nor $k$. 

Congruence (3) is a contradiction. Thus $a = b$ follows from discussion of congruence (3) and (3).

If $a = b$, then modulo $q^{2+1}$, equation (1) is

\[
(1) \ (Aq^{-1})k^{(q)} + (2) \ (Bq^{-1})k^{(q)} \equiv 0 \pmod{q}
\]

By choice, $q \neq p$ and $q$ does not divide $k$.

Thus, we have $(A + B) \equiv 0 \pmod{q}$ --- (4).

Congruence (4) shows that $B = (A + Cq)$ and thus

\[
y = (A - Aq^{-1} + Cq^{2+1})
\]

Here $C$ could be divisible by $q$ or not.

Using equation (6), $(x + y) = +Cq^{2+1}$ --- (6).

Rewrite equation (7) as

\[
y = (Dq^{-1} - x) \quad \text{and} \quad D, s \text{ are integers}. \quad \text{Then}
\]

\[
(Bq^{-1})^p = z^p = x^p + y^p = x^p + (Dq^{-1} - x)^p
\]