Fermat Triples using Modular Arithmetic

by Jim Rock

Abstract. Andrew Wiles proved there are no integers \( x, y, \) and \( z \) and a prime \( p \geq 3 \) with \( x^p+y^p+z^p=0 \). We use the Barlow relations to generate Fermat Triples where \( x^p+y^p+z^p=0 \) for an infinite number of moduli.

***

If there were positive integers \( x, y, \) and \( z \) and a prime \( p \geq 3 \), \( x^p+y^p+z^p=0 \) and \( p \) does not divide \( xyz \), the following Barlow relations must hold:

\[
x + y = t^p \quad y + z = s^p \quad x + z = s^p
\]

Solving the equations for \( x, y, \) and \( z \) gives:

\[
x = (-r^p+s^p+t^p)/2 \quad y = (r^p-s^p+t^p)/2 \quad z = (r^p+s^p-t^p)/2.
\]

We set \( r=2k+1 \), \( s =-r+2kt = -((2k+1)^p)/r \), and solve for \( t \).

\[
r^2-2kt = -(2k)^p-1/
\]

Substituting \( 2k+1 \) for \( r \) gives:

\[
4k^2 + 4k + 1 - 4k^2t - 2kt = (2k)^p+1
\]

\[
2k + 2 - 2kt - t = (2k)^p
\]

\[
(2k)^p-2k-2 = -2kt - t
\]

\[
-(2k)^p-2k-2/(2k+1) = t \quad t \text{ is always an integer for } p \geq 3.
\]

Using these formulas for \( x, y \) and \( z \) (along with the fact that \( r, s, \) and \( t \) are all congruent to zero modulo \( r \)), shows that for all primes \( p \geq 3 \), \( x^p+y^p+z^p \equiv 0 \mod (2r)^p \).

The full Barlow relations are listed in Fermat’s Last Theorem for Amateurs by Paulo Ribenboim.