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 $x^p + y^p + z^p \equiv 0$ 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:

$x + y = t^p \quad y + z = r^p \quad x + z = s^p \quad x = -rr_1 \quad y = -ss_1 \quad z = tt_1$ Solving the equations for x, y, and z gives:

$x = (-r^p + s^p + t^p)/2 \quad y = (r^p - s^p + t^p)/2 \quad z = (r^p + s^p - t^p)/2$. Substituting $-rr_1 = x$, $-ss_1 = y$, and $s = -r + 2k$, gives

$(-r^p + s^p + t^p)/2 = -rr_1 \quad (s^p + t^p)/r, \quad s = -r + 2kt, \ (-r + 2kt)^p + t^p)/r, \quad ((2k)^p + 1)/r.$
$(r^p - s^p + t^p)/2 = -ss_1, \ (r^p + t^p)/s \quad r = -s + 2kt, \ (-s + 2kt)^p + t^p)/s \quad ((2k)^p + 1)/s.$

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

$-r + 2kt = -((2k)^p + 1)/r$
$r^2 - 2ktr = (2k)^p + 1$ Substituting $2k+1$ for r gives:
$4k^2 + 4k + 1 - 4k^2t - 2kt = (2k)^p + 1$
$2k + 2 - 2kt - t = (2k)^{p-1}$
$(2k)^{p-1} - 2k - 2 = -2kt - t$
$-((2k)^{p-1} - 2k - 2) / (2k + 1) = t$ $\quad t$ 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 $p \geq 3$, $x^p + y^p + z^p \equiv 0 \bmod (2r)^p$.

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