Yet Another Fermat Paper

Ralph Muha
yafp@zerotronics.com

We analyze the difference equations between powers of successive integers to show why there is an infinity of integer solutions for $c^n = a^n + b^n$ when n = 2, and suggest a simple direction for proving that there are no integer solutions for n > 2.

Starting with the difference equation for the squares of successive integers

$$(N+1)^2 - N^2 = (N^2 + 2N + 1) - N^2 = 2N + 1 \qquad (1)$$

we can see that, for N >= 0, equation (1) produces the set of all odd integers > 0. So, if we rearrange our Fermat equation for n = 2 as

$$c^2 - b^2 = a^2 \qquad (2)$$

and choose a to be any odd integer > 1, we can use the difference equation (1) to find a pair of successive integers b and c (= b + 1), such that the difference between their squares (always an odd integer) equals a^2.

$$a = \text{any odd integer} > 1$$

$$a^2 = 2b + 1 \qquad (3a)$$

$$b = \frac{a^2 - 1}{2} \qquad (3b)$$

$$c = b + 1 \qquad (3c)$$

By substituting (3a) and (3c) into (2), we can show that

$$(b+1)^2 - b^2 = 2b + 1$$

$$b^2 + 2b + 1 - b^2 = 2b + 1$$

$$2b + 1 = 2b + 1$$

So there we have it. An (odd) infinity of integer solutions for $a^2 + b^2 = c^2$

a	b	c
3	4	5
5	12	13

7	24	25
9	40	41
11	60	61
13	84	85
15	112	113
17	144	145
19	180	181
...	...	...

Note that since a is odd and > 1, the RHS of (3b) guarantees that b will always be even, and so c will always be odd.

So, will this approach work for n > 2? The difference equation for the cubes of successive integers is

$$(N+1)^3 - N^3 = 3N^2 + 3N + 1 \quad (4)$$

If we try to compute b from a, as we did for n = 2 in (3b), we get

$$a^3 = 3b^2 + 3b + 1 \quad (5)$$

Rewriting (5) as a quadratic (6a), and applying the venerable "formula" (6b) with a bit of transformation, we arrive at (6c)

$$3b^2 + 3b + \left(1 - a^3\right) = 0 \quad (6a)$$

$$b = \frac{-3 + \sqrt{9 - 12\left(1 - a^3\right)}}{6} \quad (6b)$$

$$b = \frac{\sqrt{a^3 - 1/4}}{\sqrt{3}} - \frac{1}{2} \quad (6c)$$

which does not yield any integer solutions for a > 1 (odd or even), at least not for the first several thousand integers. But that's not a proof, simply an empirical observation. What may lead to Fermat's proof is that, for b to be an integer, the first term of the RHS of (6c) must evaluate to b + 1/2, and it is hard to see how that could happen, given that square root of (a^3 – 1/4) in the numerator and the (irrational) square root of 3 in the denominator.

So perhaps Pierre found a nice way to generalize this, for any n > 2...