

Fermat's Proof

I've heard that Fermat gave essentially one public proof of a result of his. That is a proof that $x^4 + y^4 = z^4$ has no positive integer solutions. Here is Fermat's proof.

First, Fermat actually showed that $x^4 + y^4 = z^2$ has no positive integer solutions. This includes the previous case, since, if $x^4 + y^4 = z^4$, then $x^4 + y^4 = (\text{something})^2$. Next, Fermat said that we need only consider the case where each of x, y, z is prime to the other two. To see this, suppose that d is a common divisor of x and y . We can write $x = dx_1, y = dy_1$, and so $z^2 = x^4 + y^4 = d^4x_1^4 + d^4y_1^4 = d^4(x_1^4 + y_1^4)$. Consequently, d^2 is a divisor of z , so let $z = d^2z_1$. We then have $x_1^4 + y_1^4 = z_1^2$. In this way, common factors of x and y can be removed. This means we may at least assume that x and y are relatively prime. In this case, $(x^2)^2 + (y^2)^2 = z^2$, so (x^2, y^2, z) is a Pythagorean triple in which the first two terms are relatively prime. But this means that z is prime to x^2 and y^2 , which only happens if z is prime to x and y . (To see this, suppose not. Then there is a prime p which is a common divisor of z and x^2 , say. In this case, p is a divisor of x , and with little difficulty, we see that p is also a divisor of y , which can't happen.)

So, if there are positive integer solutions to $x^4 + y^4 = z^2$, then there are solutions in which x, y, z are pairwise relatively prime. It is at this point that we start the infinite descent. We descend on z for which there are x and y , with (x, y, z) being a primitive solution to $x^4 + y^4 = z^2$. The idea is to make repeated use of our characterization of primitive Pythagorean triples to obtain an (x_1, y_1, z_1) which is primitive and satisfies $x_1^4 + y_1^4 = z_1^2$, with $0 < z_1 < z$. As in the previous paragraph (x^2, y^2, z) is a primitive Pythagorean triple. This means that one of x or y is even, and as in the past, we make the assumption that it is y that is even (we could interchange the roles of x, y if x was even.) By our characterization of Pythagorean triples, there are numbers $p > q > 0$ with

$$(1) \quad p^2 - q^2 = x^2, \quad (2) \quad 2pq = y^2, \quad (3) \quad p^2 + q^2 = z.$$

We also know that p and q are relatively prime, with one of them even. We can rewrite (1): $x^2 + q^2 = p^2$. This must be a primitive Pythagorean triple, and x is odd, so q must be even. Again, by our characterization, there are numbers

$a > b > 0$ with

$$(4) \ x = a^2 - b^2, \quad (5) \ q = 2ab, \quad (6) \ p = a^2 + b^2.$$

In addition, a and b are relatively prime, with one of them even.

Having pushed this as far as we can, we now make use of (2). Since q is even, $(2q)$ and p are relatively prime, and their product is a square. This means that each is a square. That is, there are integers c, z_1 with $2q = c^2$, and $p = z_1^2$. Since c must be even, let $c = 2d$. We have $2q = (2d)^2$ or $q = 2d^2$. We now use this idea again with (5): we have $2d^2 = 2ab$, or $ab = d^2$, and a, b are relatively prime. Thus, there are numbers x_1 and y_1 with $a = x_1^2$ and $b = y_1^2$. Finally, we plug all this into (6) to obtain

$$z_1^2 = (x_1^2)^2 + (y_1^2)^2 = x_1^4 + y_1^4.$$

Tracing through the steps, x_1, y_1 , and z_1 are mutually relatively prime, and $0 < z_1 < z$. (This is because $z_1 = p > 0$, and $z = p^2 + q^2$, with $q > 0$.) This completes the infinite descent, which shows that the equation $x^4 + y^4 = z^2$ has no primitive solutions, which in term means it has no positive integer solutions.