Math 5330
Spring 2018

Notes
Fermat's proof

I've heard that Fermat gave essentially one public proof of a result of his. That is the 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 included the previous case because if we had positive integers a, b, c with $a^4 + b^4 = c^4$, then we could let $x = a$, $y = b$, $z = c^2$ to get $x^4 + y^4 = z^2$. That is, if the sum of two forth powers can't be a square, then it certainly can't be a forth power either. Next, Fermat said that we need only consider the case where x, y, z are pairwise relatively prime. To see this, if d is a common divisor of x and y then if we let $x = dx_1$ and $y = dy_1$, we have $z^2 = x^4 + y^4 = d^4(x_1^4 + y_1^4)$, so d^2 would be a divisor of z, so writing $z = d^2 z_1$ would give $x_1^4 + y_1^4 = z_1^2$. In this way, common factors of x and y can be removed, so we can 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. This means that the third term, z, must be prime to each of these as well.

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. We now start the infinite descent. We will show that if a primitive solution exists, then there is a smaller triple (say a triple with a smaller positive z value) that is also primitive. The idea of the proof is that if (x, y, z) is a primitive solution to $x^4 + y^4 = z^2$, then (x^2, y^2, z) will be a primitive Pythagorean triple, and we have a characterization of such triples.

Here is the proof. Suppose that $x^4 + y^4 = z^2$, has solutions. As outlined above, then there is a primitive solution (x, y, z). In this case, (x^2, y^2, z) is a primitive Pythagorean triple, so one of x, y has to be even, and without loss of generality, we may let it be y. By our characterization of primitive Pythagorean triples, there are relatively prime integers p, q with

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

Moreover, one of p, q is even. We rewrite equation (1) as $x^2 + q^2 = p^2$, and since p and q have no common factors, (x, q, p) must be a primitive Pythagorean triple. Now we know that one of x^2 and q^2 is even, but x is odd, so q is even. Again by our characterization of primitive Pythagorean triples, there are relatively prime integers a, b with

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

Now we switch our attention to the equation (2). We know that q is even, p is odd, and p, q are relatively prime. This means that $2q$ is also relatively prime to p, so we have $(p)(2q) = y^2$, a square. Thus, each of p and $2q$ must be a square, so let let $p = c^2$, and $2q = d^2$. Since d must be even, write $d = 2e$, so $2q = 4e^2$, or $q = 2e^2$. We plug this into equation (5), and cancel a 2 to get $ab = e^2$, where a and b are relatively prime. Thus, each of these is also a square, $a = f^2$ and $b = g^2$. Finally, we plug all this into equation (6) giving $f^4 + g^4 = c^2$. That is, we have another solution, (f, g, c) to the equation $x^4 + y^4 = z^2$. The solution is primitive because f and g are relatively prime (because a and b are relatively prime). Since $c = p^2$, and $z = p^2 + q^2$, we have $c < z$, establishing our infinite descent.