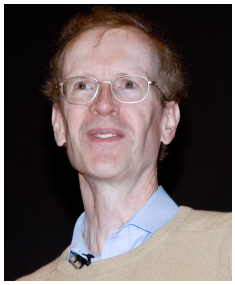


Sir Andrew John Wiles,
Abel Prize Laureate 2016

FERMAT'S LAST THEOREM FOR $n = 4$

The most prominent application of the modularity theorem is the proof of Fermat's Last Theorem. Even if Fermat claimed that he had found a marvellous proof of the statement, it is not very likely that he actually had found a proof. What we know, is that Fermat had a proof of the theorem for $n = 4$, using his proof method called infinite descent.

Diophantus of Alexandria

The case $n = 4$ is the easiest case of FLT to prove. The proof uses in a clever way a property of the positive integers, called Diophant's theorem, named after its originator, Diophantus of Alexandria (lived between 200 and 300). The theorem gives an accurate description of the so-called primitive Pythagorean triples, i.e. triples (x, y, z) of positive integers, with no common divisor, satisfying the Pythagorean equation $x^2 + y^2 = z^2$.

Diophant's Theorem. *Let x, y, z be positive integers with no common factor, and such that*

$$x^2 + y^2 = z^2$$

Then for some positive integers $p > q$, with no common factor, we can write

$$x = p^2 - q^2,\ y = 2pq,\ z = p^2 + q^2$$

We shall use this result to prove that the equation

$$x^4 + y^4 = u^2$$

has no solution among the positive integers. This is an even stronger result than the FLT for $n = 4$ by the substitution $u = z^2$.

Assume that the above equation has at least one solution, and that we consider the solution with the smallest value of u. Our first observation is that x, y, u can have no common factor, since dividing out by such a factor would produce a new solution with strictly smaller u.

To continue we observe that the equation can be written

$$(x^2)^2 + (y^2)^2 = u^2$$

and by Diophant's theorem we can find positive integers p, q with no common factor such that

$$x^2 = p^2 - q^2,\ y^2 = 2pq,\ u = p^2 + q^2$$

Another observation is that any square has remainder either 0 or 1 when divided by 4. The only way to obtain this in this case is that p is odd and q is even. So we write $q = 2c$ and we have $y^2 = 2pq = 4pc$, or $(\frac{y}{2})^2 = pc$. The next observation is that p and c are squares.

The reason for this is that since p and q have no common factor, the same is true for p and c. If we let $\frac{y}{2} = p_1 p_2 \cdot \ldots p_k$ be the prime factorization of $y/2$, we get

$$pc = (\frac{y}{2})^2 = p_1^2 p_2^2 \cdot \cdots \cdot p_k^2.$$

But p and c have no common prime factor and for each p_i either p_i^2 is a factor of p or p_i is not a factor of p. It follows that p and c are squares. Using this fact we can write $p = d^2, c = f^2$. Using $x^2 = p^2 - q^2 = (d^2)^2 - (2c)^2 = (d^2)^2 - (2f^2)^2$, we see that

$$x^2 + (2f^2)^2 = (d^2)^2.$$

It is rather straightforward to see that $x, 2f^2$ and d^2 have no common prime factor, and again using Diophant's theorem we can write

$$x = l^2 - m^2, \quad 2f^2 = 2lm, \quad d^2 = l^2 + m^2,$$

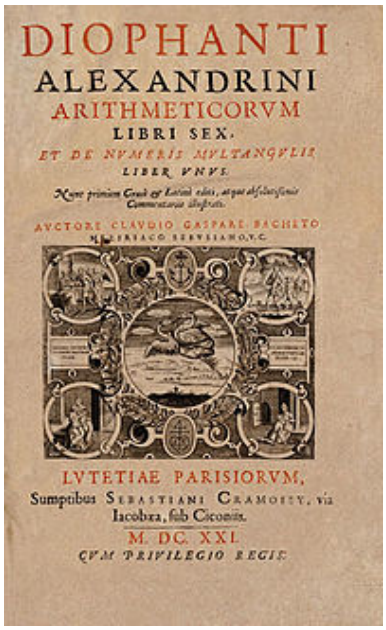
with l and m without common factor. Using the same technique as above for $f^2 = lm$, it follows that l and m are squares, i.e. $l = r^2, m = s^2$, and so

$$r^4 + s^4 = l^2 + m^2 = d^2$$

We have found a new solution of the original equation $x^4 + y^4 = u^2$, where $d < u$.

Our initial assumption was that u was the smallest right hand side among all solutions, contradicting the existence of the solution with d as the number on the right hand side. An assumption that leads to a contradiction can not be true, thus we have proved that there can not exist any positive integer solution to the Fermat equation

$$x^4 + y^4 = u^2$$



The 1621-edition of Diophantus' Arithmetica.

Diophantus is often called the *father of algebra*.