An optimization approach to Fermat's last theorem

By: Hassine Saidane, Ph.D.

Introduction to Fermat's last theorem

The so-called Fermat's last theorem is actually a conjecture that was proposed by Pierre de Fermat in 1637 regarding the Diophantine equation $x^n + y^n = z^n$, where x, y, z and n are integers, having no nonzero solution for $n > 2$. This conjecture was one of the most notable unsolved problems of mathematics. Early on, a few specific cases were proved [1]: Fermat, for $n = 4$, Euler for $n = 3$, Dirichlet and Lagrange for $n = 5$, Lamé for $n = 7$, and Dirichlet for $n = 14$. The proof was eventually extended by other mathematicians to cover all prime exponents up to four millions [2]. This conjecture was finally proven by Wiles and R. Taylor in late 1994 at the cost of long and complex analyses using new mathematical tools not accessible to the common mathematician. For his proof, Wiles received numerous awards, including the 2016 Abel Prize [2]. In this note, we present a short and accessible solution based on the following optimization approach.

Problem formulation and solution

Let's consider the function $F(x,y,z;n)$ associated with Fermat's Diophantine equation

$$D(x,y,z;n) = (x^n + y^n = z^n) \quad (1)$$

$$F(x,y,z;n) = (x^n + y^n - z^n)^2 \quad (2)$$

$F(x,y,z;n)$ has a minimum value of zero if and only if equation (1) has a solution. Hence, the task of finding out whether equation (1) has a solution or not entails analyzing the optimality of equation (2) giving that $x^{n-1} + y^{n-1} = z^{n-1}$ (e.g. $n-1 = 3$) has no solution, i.e. giving that:

$$F(x,y,z;n\text{-}1) = (x^{n-1} + y^{n-1} - z^{n-1})^2 \neq 0 \quad (3)$$

The problem of interest is then to analyze the optimality condition of the unconstrained optimization problem which is to: Minimize $F(x,y,z;n) = (x^n + y^n - z^n)$ (P)

The first order necessary optimality condition is that the gradient of F be equal to zero[1] [3], that is:

$$\frac{\partial F}{\partial x} = n\, x^{n-1} = 0; \quad \frac{\partial F}{\partial y} = n\, y^{n-1} = 0; \quad \frac{\partial F}{\partial z} = -\, n\, z^{n-1} = 0 \quad (4)$$

From (4) we get: $n\,(x^{n-1} + ny^{n-1} - z^{n-1}) = 0$, i.e. $x^{n-1} + ny^{n-1} = z^{n-1}$ (5)

Thus, for problem $D(x,y,z;n)$ to have a minimum value, it is necessary that $D(x,y,z;n\text{-}1)$ have a solution, which is in contradiction with condition (3), giving that $D(x,y,z;n\text{-}1)$ has no solution. The impossibility of this necessary condition implies that equation (1): $x^n + y^n = z^n$, can't have a solution. By induction, this result is valid for all exponents $n > 3$, thereby proving the conjecture proposed by Fermat in his last theorem.

References

1. Fermat's last theorem: https://mathworld.wolfram.com/FermatsLastTheorem.html
2. Fermat's last theorem: https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem
3. *Bertsikas, D.P., Nonlinear Programming, 2nd edition, 1995, p.4*

[1] Originally formulated by Fermat in 1637