An optimization approach to Fermat's last theorem

By: Hassine Saidane, Ph.D.

Introduction

The so-called Fermat's last theorem is actually a conjecture that was formulated by Pierre de Fermat in 1637 where he stated that the Diophantine equation $x^n + y^n = z^n$, with x, y, z and n positive integers, has no nonzero solution for $n > 2$. This conjecture was one of the most famous unsolved problems of mathematics for over three and a half centuries. Early on, the following 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 Andrew Wiles in late 1994 [2] using very long and complex analyses. In this note, we present a direct, short and easy to grasp solution based on the following optimization approach.

Problem formulation and solution

Let's consider Fermat's Diophantine equation $D(x,y,z;n)$: (1), and the associated function $F(x,y,z;n)$: (2)

$$D(x,y,z;n) = x^n + y^n = z^n \tag{1}$$

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

The Diophantine equation $D(x,y,z;n)$ has a nonzero solution if and only if $F(x,y,z;n)$ achieves a minimum value of zero for some positive integer values x, y, and z. Hence, the task of finding out whether $F(x,y,z;n)$ has a solution or not entails analyzing its optimality conditions and associated feasibility, given that $x^{n-1} + y^{n-1} = z^{n-1}$ (e.g. $n-1 = 3$) has no nonzero solution, i.e. given that:

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

Optimality conditions can be derived from the simple unconstrained optimization problem below:

$$\text{Minimize } F(x,y,z;n) = x^n + y^n - z^n \tag{P}$$

For problem (P), the necessary optimality condition is that the gradient of F be equal to zero[1] [3], that is:

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

from which we derive:

$$n\,(x^{n-1} + y^{n-1} - z^{n-1}) = 0, \text{ i.e. } x^{n-1} + y^{n-1} = z^{n-1}, \text{ since } n > 0 \tag{5}$$

Thus, in order for $F(x,y,z;n)$ to vanish, it is necessary that $D(x,y,z;n-1)$ has a solution, which is not feasible since it is in contradiction with condition (3), $D(x,y,z;n-1)$ having no solution. This infeasibility implies that the Diophantine $D(x,y,z;n) = x^n + y^n = z^n$, also has no solution. Since condition (3) is true for $n = 3$, by induction, this result is valid for all exponents $n > 3$, which proves the conjecture in Fermat's 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