An optimization approach to Fermat's last theorem

By: Hassine Saidane

Introduction to Fermat's last theorem

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 short and easy to grasp solution based on the following optimization approach.

Problem formulation and solution

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

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

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

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

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

Such conditions can be derived from the following unconstrained optimization problem which is to:

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

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

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

From (4) we get: $n\,(x^{n-1} + y^{n-1} - z^{n-1}) = 0$, hence $x^{n-1} + y^{n-1} - z^{n-1} = 0$, since $n > 0$, (5)

Thus, in order for $F(x,y,z;n)$ to vanish, it is necessary that $D(x,y,z;n\text{-}1)$ has a solution, which is in contradiction with condition (3), i.e. with $D(x,y,z;n\text{-}1)$ having no solution. The impossibility of this necessary condition implies that the Diophantine $D(x,y,z;n) = x^n + y^n = z^n$, has no solution. By induction, this result is valid for all exponents $n > 3$, thereby proving 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