

1.4.19. *Demostrar que si $2^n - 1$ es primo, n ha de ser primo.*

Solución: Supongamos que n no es primo: $n = a \cdot b$ con $1 < a, b < n$.
Observemos que el polinomio $t^a - 1$ factoriza de la siguiente manera:

$$t^a - 1 = (t - 1)(t^{a-1} + t^{a-2} + \cdots + t + 1)$$

Haciendo $t = 2^b$ obtenemos una factorización de $2^n - 1$ como producto de dos enteros estrictamente mayores que 1:

$$2^n - 1 = (2^b)^a - 1 = (2^b - 1) \cdot (2^{n-b} + 2^{n-2b} + \cdots + 2^b + 1).$$

Problema escrito por Almudena Delgado