Gauss probó mi teorema favorito: *Es posible construir con regla y compás un polígono regular con número impar n de lados si y solo si n se factoriza en primos distintos que siguen a una potencia de dos*. Es decir,

$$\begin{aligned} n &= p_1 p_2 \dots p_k \\ &= \bigl(2^{\beta_1}+1\bigr)\bigl(2^{\beta_2}+1\bigr)\dots\bigl(2^{\beta_k}+1\bigr) \end{aligned}$$

con $\beta_1, \dots, \beta_k \in \mathbb{Z}^+$ distintos.

Los tres primeros polígonos con n primo que se pueden construir son:

Nombre	**lados**	β
Triángulo	3	1
Pentágono	5	2
Heptadecágono	17	4

Se conocen solo dos más: el de $257 = 2^8 + 1$ lados y el de $65537 = 2^{16} + 1$ lados. Desconozco su nombre.

Una propiedad nada obvia es que

$$p = 2^\beta + 1 \text{ primo} \quad \Longrightarrow \quad \beta = 2^\gamma, \quad \gamma \in \mathbb{N}. \tag{1}$$

Se dice que p es un *primo de Fermat* porque Fermat conjeturó que la implicación recíproca en (1) también era cierta pero años después Euler comprobó que fallaba para $\gamma = 5$.