Lema. *Dokazati da je*

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots + a + 1)$$

za svaki realan broj a i svaki prirodan broj $k \geq 2$.

Dokaz. Direktnim računom.

Teorema (Mersenovi brojevi). *Ako je $2^n - 1$ prost broj onda je i n prost broj, za svako $n \in \mathbb{N}$.*

Dokaz. Pretpostavimo da n nije prost broj. Ako je $n = 1$ onda je $2^n - 1 = 1$, što nije prost broj. Pretpostavimo, zato, da je $n \geq 2$. Kako n nije prost broj, postoje prirodni brojevi $m \geq 2$ i $k \geq 2$ takvi da je $n = mk$. Sada je

$$2^n - 1 = 2^{mk} - 1 = (2^m)^k - 1 = a^k - 1,$$

gde smo stavili $a = 2^m$ da bismo lakše pratili nastavak dokaza. Prema Lemi je

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots + a + 1)$$

i zato je

$$2^n - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots + a + 1).$$

Kako je $a = 2^m$ i $m \geq 2$ zaključujemo da je $a - 1 \geq 3$. S druge strane iz $k \geq 2$ i $a \geq 4$ sledi da je $a^{k-1} + a^{k-2} + \ldots + a + 1 \geq 5$. Dakle, $2^n - 1$ je složen broj.