הגדרה: אם m חיובי, a זר ל-m ו-k הוא המספר הטבעי הקטן ביותר כך ש-

$a^k \equiv 1 \pmod m$ הוא $\phi(m)$ נאמר ש-a שורש פרימיטיבי מודולו m.

טענה: נניח כי $n=rs$ כאשר $(r,s)=1$ ו-a זר ל-n מתקיים

$$a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod n$$

הערה: לכל r אין שורש פרימיטיבי אם n אי זוגי ובעל לפחות שני גורמים ראשוניים אי זוגיים.

הוכחה: מספיק להראות ש-$a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod r$, $a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod s$.

לפי משפט אוילר: $a^{\phi(r)} \equiv 1 \pmod r$

$$\phi(n) = \phi(r)\phi(s)$$

$$\frac{\phi(n)}{2} = \phi(r)\underbrace{\frac{\phi(s)}{2}}_{\text{מספר אי זוגי}}$$

$$\left(a^{\phi(r)}\right)^{\frac{\phi(s)}{2}} = a^{\phi(r)\frac{\phi(s)}{2}} = a^{\frac{1}{2}\phi(n)} \equiv 1 \pmod r$$