Пусть n – произвольное целое число большее 1. Пусть s – степень вхождения двойки в $n-1$, $2m+1$ – наибольший нечетный делитель $n-1$, то есть $n-1=2^s(2m+1)$.

Свидетелем простоты числа n называется такое a из $\{2,3,\dots,n-2\}$, что

$$\begin{bmatrix} a^{2m+1} \equiv 1\ (mod\ n) \\ \exists\ t<s: a^{2^t(2m+1)} \equiv -1 (mod\ n) \end{bmatrix}$$

Теорема

Для любого простого p верно, что у 5p не больше четырех свидетелей простоты.