Es Primalità /12-05

Compito 4.1. *Testimoni e bugiardi*
Spiega per quale motivo 8 non è bugiardo per $n = 21$ anche se

$$8^{10} = 51130563 \times 21 + 1 \equiv 1 \pmod{21}$$

$n = 21$ $\quad 21 = 5 \cdot 2^2 + 1$

$q = 5$

$s = 2$

presa $a = 8$

8^5 $\xrightarrow{\times 2}$ 8^{10}

111_{21} , 111_{21}

8 $\quad +1$

8 non è un bugiardo perché, in accordo con l'algoritmo di Miller-Robin, dopo la prima iterazione (8^5) scopro che il risultato $\neq \pm 1$, dunque entro nel while, ciò significa che esco dal loop sse $x \equiv -1 \bmod n$, descrivendo "probabilmente primo" (8 bugiardo)

Ma ciò non succede in quanto il valore che ottengo è $+1$ e quindi non esco dal while ottenendo "prob primo", bensì "n composto" (come return esterno del while)