TEST DI PRIMALITÁ

- 7 é un numero primo?

↳ utilizziamo il test di Miller-Rabin per capirlo:

- $s = 0$, $q = 7 - 1 = 6$
  - $s = 1$, $q = 3$ // entro col ciclo nel primo ciclo
- $a \Rightarrow \{2, 3, 4, 5, 6\}$ ⇝ prendo $a = 2$
- $x \equiv a^q \pmod n$ ⇝ $x \equiv 2^3 \pmod n$ ⇝ $\frac{x-8}{7}$ ⇝ $x = 15$
- se $x \equiv \pm 1$ "n prob. primo" col ciclo:

  $x \not\equiv -1$ ⇝ $\frac{15+1}{7} = \frac{16}{7}$

  $x \equiv 1$ ⇝ $\frac{15-1}{7} = \frac{14}{7} = 2$ quindi "n prob. primo", esco

- Verifica che 2 é un MR-Testimone per 15 e 21:

- per ogni che 2 é un MR-Testimone per 15 e 21 mi basta prendere $a = 2$ e vedere se usando questo valore il test di Miller-Rabin restituisce per questi valori (15 e 21); "n é composto"

· 2 è un MR-testimone per 15?

· $s = 0$; $q = 15 - 1 = 14$

· $s = 1$; $q = 7$ // entro col ciclo dal primo ciclo

· $a = 2$

· $x \equiv 2^7 \rightsquigarrow \frac{x - 128}{15} \rightsquigarrow x = 143$

· $x \neq \pm 1$ // quindi vado avanti

· $s \geq 0 \rightsquigarrow 1 \geq 0$ entro una volta nel ciclo

· $x \equiv x^2 \rightsquigarrow \frac{x - 143^2}{15} \rightsquigarrow \frac{20464 - 20449}{15} \rightsquigarrow x = 20464$

· $x \neq -1$ quindi non esco $\rightsquigarrow \frac{20465}{15}$ ho resto

· esco dal ciclo quindi "n è composto", quindi (SI)

· e per 21?

· $s = 0$; $q = 21 - 1 = 20$

· $s = 1$; $q = 10$ // ancora pari devo dimezzarlo ulteriormente

· $s = 2$; $q = 5$ // ora posso uscire

· $a = 2$

· $x \equiv 2^5 \rightsquigarrow \frac{x - 32}{21} \rightsquigarrow x = 53$

· $53 \neq \pm 1$, $s = 2$ quindi [illegible] faccio ciclo

· $x \equiv 53^2 \rightsquigarrow \frac{x - 53^2}{21} \rightsquigarrow x = 2830$

· $x \neq -1 \rightsquigarrow \frac{2830 + 1}{21}$ ho resto, continuo

· $x \equiv 2830^2 \rightsquigarrow \frac{x - 2830^2}{21} \rightsquigarrow x = 8008921$

· $x \neq -1 \rightsquigarrow \frac{8008921}{21}$ ho resto, $s = 0$ quindi esco (SI)

· "n composto" dato che è l'ultima cosa che mi rimane da fare.

QUINDI

· 2 è un MR-testimone per 15 e 21