Test di Primalità di Miller-Rabin (7) Pezzano Enrico

$a = 2, 3, 4, 5$

1) $a = 2$

$s = 0$
$q = 7 - 1$
while (q pari)
$s = s + 1$ // $s = 1$
$q = q/2$ // $q = 3$

campiono a uniformemente a caso in $\{2,3,4,5\}$
$x \equiv a^q \pmod n$ // $x \equiv 2^3 \pmod 7 \equiv 1$
if $x \equiv \pm 1$ √
return 7 probabilmente primo

$a = 3$

$s = 0$
$q = 7 - 1$
while (q pari)
$s = s + 1$ // $s = 1$
$q = q/2$ // $q = 3$
$x \equiv a^q \pmod n$ // $x \equiv 3^3 \pmod 7 \equiv -1$
if ($x \equiv \pm 1$) √
return 7 probabilmente primo

$a = 4$

$s = 0$
$q = 6$
while (q pari)
$s = 1$
$q = 3$
$x \equiv 4^3 \pmod 7 \equiv 1$
if $x \equiv \pm 1$ √
return 7 probabilmente primo

$a = 5$

$s = 0$
$q = 6$
while (q pari)
$s = 1$
$q = 3$
$x \equiv 5^3 \pmod 7 \equiv -1$
if $x \equiv \pm 1$ √
return 7 probabilmente primo

$a = 6$ non viene campionato perché "si campiona a uniformemente a caso" $\{2, 3, \dots, n-2\} = \{2,3,4,5\}$

2) Verifica che 2 è un MR-testimone per 15 e 21

- $s=0$

  $q=15-1=14$

  while (q pari)

  $s=s+1=1$

  $q=q/2=7$

  $x \equiv a \pmod n \equiv 2^7 \pmod{15} \equiv 8$

  if $x \equiv \pm 1$ ×

  while $s-1 \geq 0$

  $x \equiv x^2 \pmod n \equiv 64 \pmod{15} \equiv 4$

  if $x \equiv -1 \pmod{15}$ ×

  $s=s-1=0$ // esce dal while

  return 15 composto // Siccome 15 è un n° composto, 2 è un MR-testimone

- $s=0$

  $q=21-1=20$

  while (q pari)

  $s=s+1=1$

  $q=q/2=10$ // 2° ciclo

  $s=1+1=2$

  $q=10/2=5$ // esce dal while

  $x \equiv 2^5 \pmod{21} = 11$

  if $(x \equiv \pm 1)$ ×

  while $s-1 \geq 0$

  $x = x^2 \pmod n \equiv 121 \pmod{21} \equiv 16$

  if $(x \equiv -1 \pmod{21})$ ×

  $s=1-1=1$ // 2° ciclo

  $x \equiv x^2 \pmod n \equiv 256 \pmod{21} \equiv 4$

  if $x \equiv -1 \pmod{21}$ ×

  $s=s-1=0$ // esce dal while

  return 21 composto // Siccome 21 è un n° composto, 2 è un MR-testimone