Miller-Rabin (7)

$a = 2, 3, 4, 5$

$a=2$ $s=0$

$q=6$

while (q pari)

$s=1$

$q=3$

$x \equiv 2^3 \pmod 7$

$x \equiv 1$

if $x \equiv \pm 1$ ✓

return 7 probabilmente primo

$a=3$ $s=0$

$q=6$

while (q pari)

$s=1$

$q=3$

$x \equiv 3^3 \pmod 7$

$x \equiv -1$

if $x \equiv \pm 1$ ✓

return 7 probabilmente primo

$a=4$ $s=0$

$q=6$

while (q pari)

$s=1$

$q=3$

$x \equiv 4^3 \pmod 7$

$x \equiv 1$

if $x \equiv \pm 1$ ✓

return 7 probabilmente primo

a = 5 $s = 0$

$q = 6$

while (q pari)

$s = 1$

$q = 3$

$x \equiv 5^3 \pmod 7$

$x \equiv -1$

if $x \equiv \pm 1$ ✓

return 7 probabilmente primo

a = 6 a deve essere campionata uniformemente a caso in un intervallo che va da 2 a $n-2$, quindi nel nostro caso da 2 a 5. pertanto 6 è fuori dall'intervallo di campionamento

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

$s = 0$

$q = 14$

while (q pari)

$s = 1$

$q = 7$

$x \equiv 2^7 \pmod{15}$

$x \equiv 8$

if $x \equiv \pm 1$ ✗

while $s - 1 \geq 0$

$x \equiv 64 \pmod{15}$

$x \equiv 4$

if $x \equiv -1 \pmod{15}$ ✗

$s = 0$

return 15 composto

Essendo 15 un numero composto 2 è un MR-testimone

$s=0$

$q=20$

while (q pari)

$s=1$

$q=10$

$s=2$

$q=5$

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

$x \equiv 11$

if $x \equiv \pm 1$ X

while $s-1 \geq 0$

$x \equiv 121 \pmod{21}$

$x \equiv 16$

if $x \equiv -1 \pmod{21}$ X

$s=1$

$x \equiv 256 \pmod{21}$

$x \equiv 4$

if $x \equiv -1 \pmod{21}$ X

$s=0$

return 21 composto

Essendo 21 un numero composto 2 è un MR-testimone.