Batti Bobste

1) Miller - Rabin

$s=0$

$q=7-1$

while(q pari)

$s=s+1$ // $s=1$

$q=q/2$ // $q=3$

campiona a un farmeuente a caso in $\{2,3,4,5\}$

$x \equiv a^q \pmod n$ // $x \equiv 2^3 \pmod 7$ $\quad x \equiv 1$

if $x \equiv \pm 1$

return 7 probabilmente primo

$s=0$

$q=7-1$

while(q pari)

$s=s+1$ // $s=1$

$q=q/2$ // $q=3$

$x \equiv a^q \pmod n$ // $x \equiv 3^3 \pmod 7$ $\quad x \equiv -1$

if $x \equiv \pm 1$

return 7 probabilmente primo

$s=0$

$q=7-1$

while(q pari)

$s=s+1$ // $s=1$

$q=q/2$ // $q=3$

$x \equiv a^q \pmod 7$ // $x \equiv 4^3 \pmod 7$ $\quad x \equiv 1$

if $x \equiv \pm 1$

return 7 probabilmente primo

$s=0$

$q=7-1$

while(q pari)

$s=s+1$ // $s=1$

$q=q/2$ // $q=3$

$x \equiv a^q \pmod 7$ // $x \equiv 5^3 \pmod 7$ $\quad x \equiv -1$

if $x \equiv \pm 1$ return 7 probabilmente primo

per 6 non vale fatto in quanto come già segnalato, "a" campiona a uniformemente a caso in $\{2, 3 \dots, \underbrace{n-2}_{5}\}$

2) MR-testimone

$s=0$
$q=n-1$ // $q=15-1$
while (q pari)
$s=s+1$ // $s=1$
$q=q/2$ // $q=7$
$x \equiv a^q \pmod n$ // $x \equiv 2^7 \pmod{15}$ $x \equiv 128 \bmod 15$ $x \equiv 8$
if $x \equiv \pm 1$ 15 non è primo
while $s-1 \geq 0$
$x \equiv x^2 \pmod n$ // $x \equiv 8^2 \pmod{15}$ $x \equiv 4$
if $x \equiv -1 \pmod n$ 15 non è primo

$s=0$

return 15 composto

Quindi poniamo definire che 2 è MR-testimone per 15

$s=0$
$q=n-1$ // $q=21-1$
while (q pari)
$s=s+1$ // $s=1$
$q=q/2$ // $q=10$
$x \equiv a^q \pmod n$ // $x \equiv 2^{10} \pmod{21}$ $x \equiv 16$
if $x \equiv \pm 1$ 21 non è primo
while $s-1 \geq 0$
$x \equiv x^2 \pmod n$ // $x \equiv 16^2 \pmod{21}$ $x \equiv 4$
if $x \equiv -1 \pmod n$ 21 non è primo

$s=0$

return 21 composto

Perciò ne traiamo che 2 è MR-testimone anche per 21