ESEMPIO 1

n=900900900900900900900900900900900900900900900900900900901
seems prime after 10 tests.
pseudoprimo.

n-1=900*1001001001001001001001001001001001001001001001001001001

=900*21319*46953468783761011351423659693278343308832543787279
=900*21319*10749631*4367914469227921530648229664188318958002609
= 900*21319*10749631*1111111111111111111*3931123022305129377976519

M=4367914469227921530648229664188318958002609=
1111111111111111111 * 3931123022305129377976519
intero composto, completamente fattorizzato, > sqrt(n)

Applichiamo Pocklington:

M=p*q
p=1111111111111111111
q=3931123022305129377976519

```
x=lift(mod(random,n)^((n-1)/M))
mod(x,n)^M
gcd(lift(mod(x,n)^(M/p))-1,n)
gcd(lift(mod(x,n)^(M/q))-1,n)
```

```
x=lift(mod(17,n)^((n-1)/M))
=57042581758450462090658347954327144025333886774507129873
mod(x,n)^M=1
gcd(lift(mod(x,n)^(M/p))-1,n)=1
gcd(lift(mod(x,n)^(M/q))-1,n)=1
```

CONCLUSIONE:
n=900900900900900900900900900900900900900900900900900900901
PRIMO

==

ESEMPIO 2

n=10000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000949
seems prime after 10 tests.
pseudoprimo.

n-1=
476*21008403361344537815126050420168067226890756302521008403361344537815126050420168067226890756302523

=476*1805003*11638985287749958207895527276225062909530209258666610749877614905800780414448157741137765841
=476*1805003*10284191*1131735620988559839845013309868035600421093818528517289291653072740556881377267083151

R=113173562098855983984501330986803560042109381852851728929165307274055688 1377267083151
e' composto, ma "non riusciamo a fattorizzarlo".

FINE della storia.

==

ESEMPIO 3

n=10000000000000000000000000000000000000000000000000000000000093
pseudoprimo

n-1=2^2 * 3 * 2621 * 66037 * 3397567 * 1417086523103994077407747247360614547699381699

R=1417086523103994077407747247360614547699381699
pseudoprimo

Prendiamo M=R e calcoliamo
x=lift(mod(random,n)^((n-1)/R))
mod(x,n)^R
gcd(x-1,n)

x=lift(mod(2,n)^((n-1)/R)
=7177493323391307598818294406496164465181399154046999462613725
mod(x,n)^R = 1
gcd(7177493323391307598818294406496164465181399154046999462613725 - 1, n) = 1

R primo =====> n primo

Adesso applichiamo il criterio di Pocklington ad R

R=1417086523103994077407747247360614547699381699
pseudoprimo

R-1=Q*S=(2 * 59 * 919 * 385792526683)* 33872327408997649981423214143

S=33872327408997649981423214143
pseudoprimo

Prendiamo M=S e calcoliamo
x=lift(mod(random,R)^((R-1)/S))
mod(x,R)^S
gcd(x-1,R)

x=lift(mod(2,R)^((R-1)/S))=94942944984654891169014506822567050827971839 8
mod(x,R)^S=1
gcd(x-1,R)=1

S primo =====> R primo =====> n primo

Adesso applichiamo il criterio di Pocklington ad S

S=338723274089976499814232141 43
pseudoprimo

S-1=Q*T=(2 * 3 * 137 * 3701) * 11134074833788477626361

T=11134074833788477626361
pseudoprimo

Prendiamo M=T e calcoliamo
x=lift(mod(random,S)^((S-1)/T))
mod(x,S)^T
gcd(x-1,S)

x=lift(mod(5,S)^((S-1)/T))=98633670384365718948235723 36
mod(x,S)^T=1
gcd(x-1,S)=1

T primo =====> S primo =====> R primo =====> n primo

Adesso applichiamo il criterio di Pocklington a T

T=11134074833788477626361
pseudoprimo

T-1=Q*U=(360*201389)*153573361253159
U=153573361253159 pseudoprimo

Prendiamo Prendiamo M=U e calcoliamo
x=lift(mod(random,T)^((T-1)/U))
mod(x,T)^U
gcd(x-1,T)

x=lift(mod(19,T)^((T-1)/U))=62719504646652672053 60
mod(x,T)^U=1
gcd(x-1,T)=1

U primo ====> T primo =====> S primo =====> R primo =====> n primo

---

A questo punto

U=153573361253159 pseudoprimo
e' abbastanza piccolo da poter essere completamente fattorizzato:
U e' PRIMO.

CONCLUSIONE: n e' primo.