TEST DI PRIMALITA' DI POKLINGTON: ESEMPI

Due mini esempi per illustrare il test di primalita' di Pocklington.
Sia **n** l'intero da esaminare. Per poter applicare il test di Pocklington e' necessario produrre un primo (o almeno pseudoprimo) Q maggiore di radice di **n** che divide **n-1.**

Poiche' gli interi a cui si applicano i test di primalita' hanno un ordine di grandezza che va ben oltre i record di fattorizzazione ed **n-1** ha lo stesso ordine di grandezza di **n**, puo' succedere che una fattorizzazione anche parziale di **n-1** risulti impossibile. In tal caso non si puo' piu' procedere e il test di Pocklington non puo' essere applicato.

==

ESEMPIO 1

n=1000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000949
seems prime after 10 tests.
pseudoprimo.

n-1=
476*210084033613445378151260504201680672268907563025210084
03361344537815126050420168067226890756302523
=476*1805003*116389852877499582078955272762250629095302092
586666107498776149058007804144481577411377765841
=476*1805003*10284191*113173562098855983984501330986803560
0421093818528517289291653072740556881377267083151

R=1131735620988559839845013309868035600421093818528517289
291653072740556881377267083151
e' composto, ma "non riusciamo a fattorizzarlo" neanche parzialmente.

FINE.

==

======

ESEMPIO 2

n=1000000000000000000000000000000000000000000000000000000000000093
pseudoprimo

n-1=2^2 * 3 * 2621 * 66037 * 3397567 * 14170865231039940774077472473606145476993816 99

R=14170865231039940774077472473606145476993816 99
pseudoprimo

Calcoliamo
x=lift(Mod(random,n)^((n-1)/R)))
Mod(x,n)^R
gcd(x-1,n)

oppure, ad esempio,

x=lift(Mod(2,n)^((n-1)/R))
=717749332339130759881829440649616446518139915404699946261372 5
Mod(x,n)^R = 1
gcd(717749332339130759881829440649616446518139915404699946261372 5 - 1, n) = 1

R primo =====> n primo

Adesso applichiamo il criterio di Pocklington ad R

R=14170865231039940774077472473606145476993816 99
pseudoprimo

R-1=Q*S=(2 * 59 * 919 * 385792526683)* 338723274089976499814232141 43

S=338723274089976499814232141 43
pseudoprimo

Calcoliamo
x=lift(Mod(random,R)^((R-1)/S))
Mod(x,R)^S
gcd(x-1,R)

oppure, ad esempio,

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

Calcoliamo
x=lift(Mod(random,S)^((S-1)/T))
Mod(x,S)^T
gcd(x-1,S)

oppure, ad esempio,

x=lift(Mod(5,S)^((S-1)/T))=9863367038436571894823572336
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

Calcoliamo
x=lift(Mod(random,T)^((T-1)/U))
Mod(x,T)^U
gcd(x-1,T)

oppure, ad esempio,

x=lift(Mod(19,T)^((T-1)/U))=6271950464665267205360
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.