Test af faktorisering (vedr. RSA kryptering)

restart

Man kan med Maple let fremskaffe 2 store primtal t1 og t2.
Gøres ved at anvende "nextprime" på et stort tal, man selv opdigter.
"nextprime" angiver det første primtal som er større end argumentet i parentes.

$t1 := nextprime(491037684922309735353543 4) = 491037684922309735353543 7$

$t2 := nextprime(193745218693225126324554 8181) = 193745218693225126324554 8191$

Nu kan man danne produktet p af de 2 store primtal:

$p := t1 \cdot t2 = 95136203651887873899979744731756619690844450097444 67$

I RSA-kryptering skal man knække koden ved at beregne disse 2 primtal.

Maple har en rutine "ifactor" til opløsning i primfaktorer.
Anvender den og måler den forbrugte tid (i sekunder):

$tid1 := time(\,) : Primfaktorer := ifactor(p) : tid2 := time(\,) : ForbrugtTid := tid2 - tid1 :$

$Primfaktorer = (491037684922309735353543 7)\,(193745218693225126324554 8191)$

$ForbrugtTid = 1.047$

Dvs. p er opløst i primfaktorer på ForbrugtTid i sekunder (som afhænger af computeren).

De 2 tal i paranteserne er de 2 primtal givet foroven!