```
pmod(a,k,m)
Func

Local  x_,k_

k→k_:1→x_:a→pot:
Loop
 If mod(k_,2)=1 Then
   mod(x_*pot,m)→x_
   If k_=1 Then
     Return  x_
     Exit
   EndIf
   k_-1→k_
 EndIf
 k_/2→k_
 mod(pot*pot,m)→pot
EndLoop
EndFunc
```

MuPAD powermod(a,k,m)

PowerMod

MuPAD powermod(a,k,m) dient dazu, die **Potenzierung im Modul** so geschickt zu machen, dass die zu hantierenden Zahlen nicht größer als das Quadrat des Moduls werden.

Die Idee basiert auf der "Doubbeldaddel"-Methode zur Erzeugung von Dualzahlen. Die Hilfsvariable pot nimmt nacheinander die Werte

$a, a^2, \left(a^2\right)^2, \left(\left(a^2\right)^2\right)^2, \ldots$ an.

Bei ungeraden Zwischenergebnis k_ wird das bisher Erreichte mit pot multipliziert, bei geradem nicht. Stets wird sofort der Rest modulo m gebildet. Ein ungerades k_ wird um 1 reduziert, ein gerades nicht. Das neue k_ ist die Hälfte davon.

```
ordo(a,m)
Func
Local  ordn,pot
1→ordn:mod(a,m)→pot:
If gcd(a,m)>1 Then
   Return  "fail":Return
:EndIf:
Loop
  If pot=1 Then
    Return  ordn: Exit:
EndIf:
   mod(pot*a,m)→pot:
ordn+1→ordn:
EndLoop:
EndFunc
```

Ordnung eines Elementes

$\mathbb{Z}_m^*$ ist Gruppe. Für Elemente a endlicher Gruppen ist die "Ordnung von a" der kleinste Exponent von a, der $a^k = 1$ erzeugt.

Idee: einfach durchforsten, immer mehr a-Faktoren, wenn 1 herauskommt, wird der Exponent ausgegeben.

MuPAD numlib::order(a,m)

Ti-Connect, Device-Explorer, krypto, functions, Dateien markieren, actions, Copy to PC. Graph-Link für ti92, im Programme-Fenster klicken, Datei, öffnen *.* wählen, (nicht was von selbst da steht nehem!!!!), die gewünschte Datei doppelklicken, Dann steht sie im Programme-Fenster. Markieren, in Textverarbeitung stellen, Markieren, Schrift TI-Math wählen.