Kryptografie Miller-Rabin Primzahltest

```
Define LibPub istprim(n,wmax)=
Func
:Local w,k,a,m,z,zw
:If mod(n,2)=0 Then
:   Return false
:EndIf
:zw:=zweiraus(n-1)
:k:=zw[2]: w:=0
:Lbl a_wahl
:If w=wmax Then
:   Return true
:EndIf
:a:=randInt(2,n-2)
:If  not  gcd(a,n)=1 Then
    return false
:EndIf
:If kry\pmod(a,n-1,n)=1 Then
:   w:=w+1: Goto a_wahl
:Else
:   Return false
: EndIf
:z:=kry\pmod(a,zw[1],n)
:If mod(z,n)=1 or mod(z,n)=−1 Then
:    w:=w+1: Goto a_wahl
:EndIf
: m:=0
:Lbl quad
:  z:=mod(z^(2),n): m:=m+1
:If mod(z,n)=1 Then
:    Return false
:EndIf
:If mod(z,n)=−1 Then
:   w:=w+1: Goto a_wahl
:EndIf
:If m+1=k Then
:   w:=w+1: Goto a_wahl
:Else
:   Goto quad
:EndIf
:EndFunc
```

```
Define LibPub zweiraus(n)=
Func
:Local z,k
:k:=0:z:=n
:While mod(z,2)=0
:  z:=((z)/(2)):   k:=k+1
:EndWhile
:Return {z,k}
:EndFunc
```

Wenn die Funktion istprim(n,wmax) true liefert, dann ist n mit einer Irrtumswahrscheinlichkeit von mindestens $\frac{1}{2^{\text{wmax}}}$ eine Primzahl.

Wenn die Funktion istprim(n,wmax) false liefert, dann ist n sicher zusammengesetzt.

Die Funktion **zweiraus(m)** zieht aus m in die maximale Potenz von 2 heraus, Ergebnis {d,k}
zweiraus(15*2^4) ergibt die Liste {15,4}

Kernidee $n-1=d\cdot 2^k$ und mit k Quadrierungen

$$a^{n-1}=\left(\left(\left(a^d\right)^2\right)^2\ldots\right)^2$$

Da für eine Primzahl p gilt: $a^{p-1}\underset{p}{\equiv}1$ (Kl. Fermat-Satz) und

$x^2\underset{p}{\equiv}1 \Leftrightarrow x\underset{p}{\equiv}1 \vee x\underset{p}{\equiv}-1$, es gibt nur zwei Einheitswurzeln. Man sucht bei a^d und den nachfolgenden Quadrierungen nach 1 und -1. Dabei nutzt man aus, dass nach der ersten Quadrierung -1 zuerst auftreten muss, da es sonst eine weitere Einheitswurzel gibt. In dem Fall ist n sicher zusammengesetzt.

Starke Pseudoprimzahlen könnten diesen Test für das zufällige a bestehen, aber nicht für jedes a.

```
istprim(101,4) ▸ true
istprim(781,1) ▸ false
istprim(561,2) ▸ true
istprim(561,4) ▸ false
isPrime(561) ▸ false
```

Darum werden mehrere a gewählt. 781 ist so eine Zahl, das zufällige a war aber nicht 5, 17 …, eine der gefährlichen Basen.
Die Carmichaelzahl 561 ist hier zweimal falsch beurteilt, aber bei mehreren a-Wahlen (durch die 4 angezeigt) kann sie als zusammengesetzt erkannt werden.
Da Carmichaelzahlen nachweisbar weitere Einheitswurzeln besitzen, können Sie diesen Test nicht für jedes a bestehen.

Diese und die Wahrscheinlichkeitsaussage sind aus
Rempe, Lasse; Waldecker, Rebecca
Primzahltests für Einsteiger
Wiesbaden, 2009