Ist 2^n mod 2 = 2 ein Primzahl-Test?

Mathematik mit MuPAD 3.11, Prof. Dr. Dörte Haftendorn überarbeitet Sept. 05

Web: www.uni-lueneburg.de/mathe-lehramt www.uni-lueneburg.de/ing-math

Achtung: Menu ->Notebook->Evaluiere->Alle Eingaben

Wenn p prim, dann ist $2^{p-1} \equiv_p 1$ *also* $2^p \equiv_p 2$.

Kleiner Fermatscher Satz

Gilt das auch umgekehrt? Antwortversuch in Einfach-Programmierung, Suche auch in anderen Bereichen. Erwickle eine bessere Prozedur.

```
• test:=n->if powermod(2,n,n)=2 then factor(n)else ""
  end_if
                n -> (if powermod(2, n, n) = 2 then
                    factor(n)
                  else
                    ""
                  end_if)
• test(n)$ n=1..1000;

.... "", 3, "", 5, "", 7, "", "", "", 11, "", 13, "",
"", "", 17,.........ganz viele Primzahlen, aber auch:

   "", 11 31, .......", "", 3 11 17, "", 563,......
"", 1999, ""
```

• 11*31; 2^% mod % • 341 2 • 3*11*17; 2^% mod % 561 2	• 3*5*43; 2^% mod % 645 2 3*13*17;	• 7*13*19; 2^% mod % 1729 2 • 3*5*127; 2^% mod % 1905 2

Also sind bis 2000 mind. 7 Ausnahmen gefunden worden.

Wenn $2^n \equiv_n 2$ **, dann folgt nicht unbedingt, dass n prim ist.**

Dies ist also kein Primzahltest.

Es lohnt sich aber weitere Prüfungen erst anzustellen,

wenn 2^n mod n =2 ist.

Diese Bedingung ist notwendig aber nicht hinreichend.