Einfache Primzahltests

Satz: Wenn *n eine Primzahl ist, so gilt*

$$a^{n-1} \equiv 1 \bmod n$$

für alle $a \in \{1, 2, \ldots, n-1\}$.

```
FermatPT[n_Integer /; n ≥ 3,
  m_: 10] := Block[{i, a},
  For[i = 1, i ≤ m, i++,
   Block[
    {a = Random[Integer, {2, n - 1}]},
    If[PowerMod[a, n - 1, n] ≠ 1,
     Block[{},
      Print[n,
       " ist zusammengesetzt."];
      Return[a]]]]];
  Print[n,
   " ist wahrscheinlich prim."];
  Null
 ]
```

```
FermatPT[
 9106410987412061203948712346 3]
```

```
9106410987412061203948712346 3
  ist zusammengesetzt.
```

48328629040756225295633730331

```
GCD[9106410987412061203948712346 3,
    48328629040756225295633730331]
```

1

```
FermatPT[1729, 2]
```

1729 ist wahrscheinlich prim.

```
FermatPT[1729, 5]
```

1729 ist zusammengesetzt.

182

```
GCD[1729, 182]
```

91

```
Prime[10^9]
```

22801763489

```
FermatPT[22801763489]
```

22801763489 ist wahrscheinlich prim.

```
n =
  37471085616019834612091872365101 23:
   09871234761460129841260142098412 0:
   91231234701923466019102980012894 6:
   10239651098237409612034987123409 8:
   16231297864129874519781234691234 5:
   12987142349871253987169874123412 3:
   09823456109834710936614098712309 6:
   12098714460198461029384610984656 1:
   0918344019283;
Timing[FermatPT[n]]
```

```
37471085616019834612091872365101230987123 47:
  61460129841260142098412091231234701923466:
  01910298001289461023965109823740961203498:
  71234098162312978641298745197812346912345:
  12987142349871253987169874123412309823456:
  10983471093661409871230961209871446019846:
  10293846109846561091834401928 3
  ist zusammengesetzt.
```

```
{1.73 Second,
 33735147389624345286408255398198191:
  08847697770775495061009025703680214:
  51577447793946242129199690167048167:
  89349575678310478067499518407574311:
  77113822132659840989128833817718763:
  24886405925252764279640590797586318:
  40604103065189327889592377669002413:
  06762836698570015906272732371618}
```

```
GCD[n,
 33735147389624345286408255539819819⋱
  10884769777077549506100902570368 02⋱
  14515774477939462421291996901670 48⋱
  16789349575678310478067499518407 57⋱
  43117711382213265984098912883381 77⋱
  18763248864059252527642796405907 97⋱
  58631840604103065189327889592377 66⋱
  90024130676283669857001590627273 23⋱
  71618]
```

1