# Fermat-Primzahltest

**Eingabe:** $n \in \mathbb{N}$, $n \geq 3$ und $m \in \mathbb{N}$

**Ausgabe:** *zusammengesetzt*, falls $n$ eine zusammengesetzte Zahl ist; sonst *wahrscheinlich prim*.

FERMATPT($n$, $m$)

(1) $W :=$ Menge von $m$ zufälligen Zahlen aus $[2, n-1]$;
(2) **foreach** $a \in W$ **do**
(3) **if** $a^{n-1} \not\equiv 1$ mod $n$ **then**
(4) **print** „zusammengesetzt“;
(5) **return** $a$
(6) **end**
(7) **end**
(8) **print** „wahrscheinlich prim“;