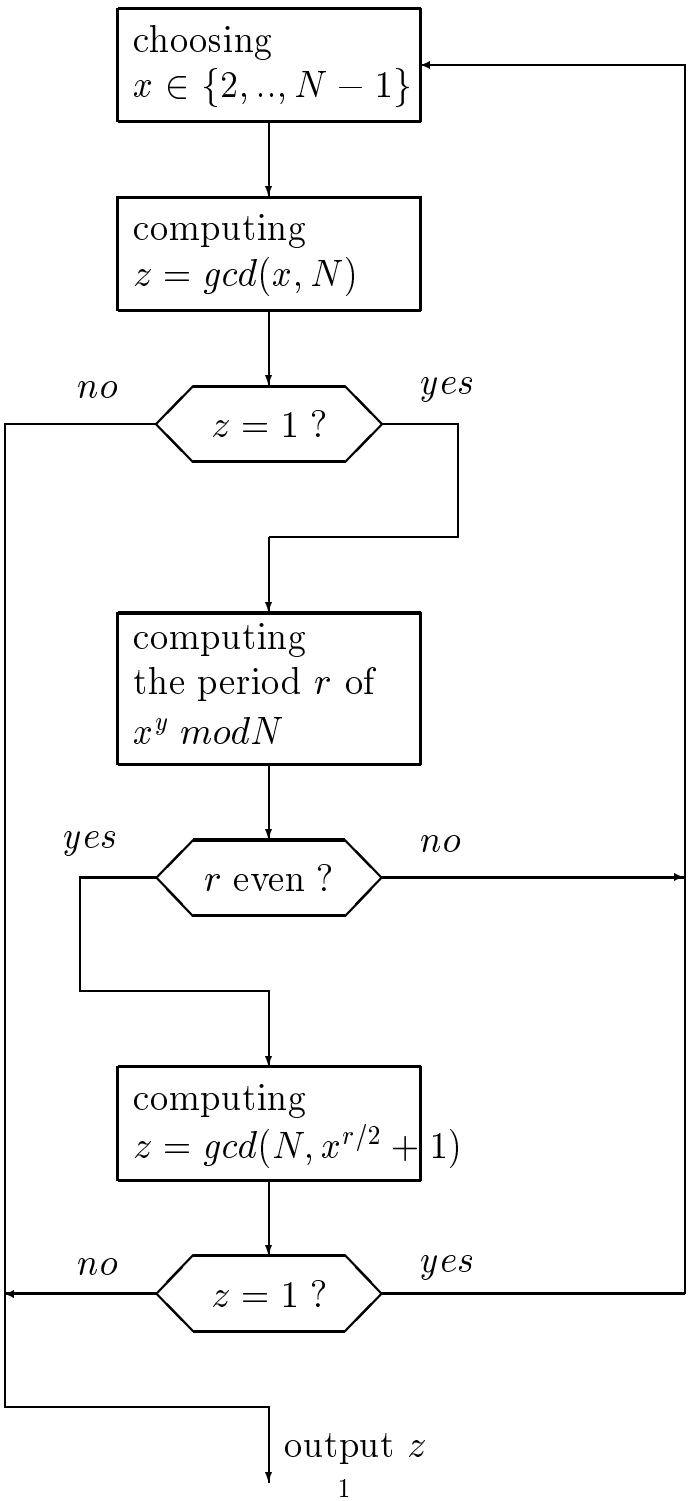
choosing
$x \in \{2, .., N-1\}$
computing
$z = gcd(x, N)$
no
$z = 1$?
yes
computing
the period r of
$x^y \; mod N$
yes
r even ?
no
computing
$z = gcd(N, x^{r/2} + 1)$
no
$z = 1$?
yes
output z