

Description of the algorithm:

input: integers b, m (modulus)

output: inverse of b modulo m

$f(x) = (bx \bmod m) - 1$, variables: y_1, y_2, x_1, x_2, l_1

1.

$y_1 = f(1)$,

$y_2 = f(2)$,

2.

$i = 3$,

while($|f(i) - y_1| > 12$), $i = i + 1$

3.

$x_1 = x$,

$l_1 = y_2 - y_1$,

4.

$j = 1$,

while($f(j) \bmod l_1 \neq 0$), $j = j + 1$

5.

$x_2 = j - 1$,

return $x_2 - x_1 \frac{bx_2 \bmod m}{l_1}$