

MODULAR-LINEAR-EQUATION-SOLVER(a, b, n)

1 $(d, x', y') = \text{EXTENDED-EUCLID}(a, n)$

2 **if** $d \mid b$

3 $x_0 = x'(b/d) \bmod n$

4 **for** $i = 0$ **to** $d - 1$

5 print $(x_0 + i(n/d)) \bmod n$

6 **else** print “no solutions”