FINDING AN INVERSE OF N (mod n)

GIVEN INTEGERS N and n such that gcd(N,n) = 1, an INVERSE OF N (mod n) is an integer s such that $Ns \equiv 1 \pmod{n}$.

If $\gcd(N,n) \neq 1$, then no such integer s exists!

If $\gcd(N,n) = 1$, then such an integer s exists!

Assuming that $\gcd(N,n) = 1$,

perform the process to express the gcd (which equals 1 here) as

$$1 = Ns + nt.$$

① The integer s is an INVERSE OF N (mod n)

and ② If x is any other integer such that $x \equiv s \pmod{n}$, then x is also an inverse of N (mod n).

EXAMPLE: Let N = 60 and n = 7. FIND AN INVERSE OF 60 (mod 7). [Sol'n: s = 2 is an inverse of 60 (mod 7)]

Perform the process to get $1 = (60)(2) + (7)(-17)$

Let s = 2. $Ns \equiv 1 \pmod{7}$:

$(60)(2) \equiv 1 \pmod{7}$ since $[1 - (60)(2)] = (7)(-17)$

so $7 \mid [1-(60)(2)] = (1-Ns)$, so $(60)(2) \equiv 1 \pmod{7}$