SOLVING SIMPLE CONGRUENCES, $Bx \equiv D \pmod n$, when $\gcd(B,n) = 1$

Assume that n and all other variables used here are integers and assume that $n > 1$. Suppose B and n are relatively prime, and so $\gcd(B,n) = 1$.

Let A be one of the $(\bmod n)$ inverses of B; that is, $AB \equiv 1 \pmod n$ and $BA \equiv 1 \pmod n$.

Consider the congruence $Bx \equiv D \pmod n$.

Suppose $x = x_0$ is a solution of this congruence; so, "$Bx_0 \equiv D \pmod n$" is a True Statement.

Suppose $x_1 \equiv x_0 \pmod n$. Then, by Theorem 8.4.3, $Bx_1 \equiv Bx_0 \equiv D \pmod n$; that is, $Bx_1 \equiv D \pmod n$.

Thus, $x = x_1$ is another solution of this congruence.

By Theorem (N1B) 4, $(x_0 \bmod n) \equiv x_0 \pmod n$, so $(x_0 \bmod n)$ is another solution; in fact, $(x_0 \bmod n)$ is the least non-negative solution of the congruence, and the solution set of "$Bx \equiv D \pmod n$" is $[\mathbb{Z}]$, where $[\mathbb{Z}]$ is the "$\equiv \pmod n$" congruence class containing $\mathbb{Z}$, and $\mathbb{Z}$ is any solution of "$Bx \equiv D \pmod n$".

RECALL THAT A is a $(\bmod n)$ inverse of B, so that $AB \equiv 1 \pmod n$. MULTIPLY "$Bx \equiv D \pmod n$" by A on both sides. By Thm 8.4.3, $A(Bx) \equiv AD \pmod n$, but $A(Bx) \equiv (AB)x \equiv 1x \equiv x \pmod n$. So, $x \equiv A(Bx) \equiv AD \pmod n$, that is, $x \equiv AD \pmod n$.

TO VERIFY THAT $x = AD$ is one solution, note that $B(AD) \equiv (BA)D \equiv 1 \cdot D \pmod n$

THUS, $(AD \bmod n)$ is the least non-negative solution and the solution set is $[AD]$.

EXAMPLE CONGRUENCE AND SOLUTION

Consider the congruence $99x \equiv 5 \pmod{13}$.

$99 = 3^2 \times 11$, so $\gcd(99, 13) = 1$.

So, (mod 13) inverses of 99 exist.

With some effort, we can discover that

31 is a (mod 13) inverse of 99, that is,

$(31)(99) \equiv 1 \pmod{13}$. To check, we calculate

$(31)(99) = (13)(236) + 1$.

We now multiply both sides of the congruence by 31, a (mod 13) inverse of 99: $(31)(99x) \equiv (31)(5) \pmod{13}$, which remains true by Theorem 8.4.3.

Also, $(31)(99x) \equiv ((31)(99))x \equiv 1 \cdot x \equiv x \pmod{13}$,

So, $x \equiv (31)(99x) \equiv (31)(5) \equiv 155 \pmod{13}$.

Thus "$x \equiv 155 \pmod{13}$" will be true about every solution of the congruence.

So, $x = 155$ is one solution. Check: $(99)(155) = (13)(1180) + 5$

So, $(99)(155) \equiv 5 \pmod{13}$ by Thm 8.4.1.

Since 155 is a solution,

$(155 \bmod 13) = 12$ is the least non-negative solution.

CHECK: $(99)(12) = (13)(91) + 5$, so $(99)(12) \equiv 5 \pmod{13}$.

The solution set for "$99x \equiv 5 \pmod{13}$" is $[12] = [155]$

The Solution Set is

$$\{\ldots, -27, -14, -1, 12, 25, 38, \ldots, 142, 155, 168, \ldots\}$$

Problem: Solve the congruence $125x \equiv 47 \pmod{216}$

Sol'n: We need to show that $\gcd(125, 216) = 1$

$$216 = 1(125) + 91$$
$$125 = 1(91) + 34$$
$$91 = 2(34) + 23$$
$$34 = 1(23) + 11$$
$$23 = 2(11) + 1$$
$$11 = 11(1) + 0$$

$\gcd(125, 216) = 1$

$91 = (1)(216) - (1)(125)$

$34 = (1)(125) - (1)(91)$

$23 = (1)(91) - (2)(34)$

$11 = (1)(34) - (1)(23)$

$1 = (1)(23) - (2)(11)$

$1 = (1)(23) - (2)[(1)(34) - (1)(23)]$

$1 = (1)(23) - (2)(34) + (2)(23)$

$1 = (3)(23) - (2)(34)$

$1 = (3)[(1)(91) - (2)(34)] - (2)(34)$

$1 = (3)(91) - (6)(34) - (2)(34) = (3)(91) - (8)(34)$

$1 = (3)(91) - (8)[(1)(125) - (1)(91)]$

$1 = (3)(91) - (8)(125) + (8)(91)$

$1 = (11)(91) - (8)(125)$

$1 = (11)[(1)(216) - (1)(125)] - (8)(125)$

$1 = (11)(216) - (11)(125) - (8)(125) = (11)(216) - (19)(125)$

So, $1 = (11)(216) + (-19)(125)$

Therefore, by Theorem 8.4.1, $1 \equiv (-19)(125) \pmod{216}$

$(-19) \equiv (-19) + 216 \pmod{216}$

$\therefore -19 \equiv 197 \pmod{216}$

$\therefore (-19)(125) \equiv (197)(125) \pmod{216}$

$\therefore (197)(125) \equiv 1 \pmod{216}$

$\therefore (197)$ is a $(\mathrm{mod}\ 216)$ inverse of 125.

From $125x \equiv 47 \pmod{216}$, we get

$(197)(125)x \equiv (197)(47) \pmod{216}$

and $(197)(125)x \equiv 1 \cdot x \equiv x \pmod{216}$.

$\therefore x \equiv (197)(47) \pmod{216}$

$\therefore (197)(47)$ is one solution.

Since $(197)(47) = (216)(42) + 187$ and $0 \leq 187 < 216$,

$((197)(47) \bmod 216) = 187$ by definition of the "mod" function

$\therefore x = 187$ is the least non-negative solution of the congruence $125x \equiv 47 \pmod{216}$.

The solution set of the congruence is

$[187] = \{\ldots, -245, -29, 187, 403, \ldots\}$

Check: $(125)(187) = 23{,}375$

$23{,}375 = (216)(108) + 47$, so $23{,}375 \equiv 47 \pmod{216}$

So, $(125)(187) \equiv 47 \pmod{216}$.