Solving Simple Congruences, $B \cdot x \equiv D \pmod{n}$, when $\gcd(B, n) = 1$

In this paper, $A$, $B$, $C$, $D$, and $n$ represent any integers such that $n > 1$ and $\gcd(B, n) = 1$.

The variable $x$ represents an integer such that the statement $B \cdot x \equiv D \pmod{n}$ is a true statement, that is, $x$ is a solution of the congruence. To "solve the congruence" means to determine its solution set, that is, the set of all solutions of the congruence. Also, if $x_0$ is one particular solution of the congruence, then any other integer $y$, such that $y \equiv x_0 \pmod{n}$, is also a solution.

Let $A$ be a $(\mod{n})$ inverse of $B$. It will shown that $x = AD$ is a solution of the congruence above.

By Theorem (NIB) 4, $AD \equiv (AD \mod{n}) \pmod{n}$, so $x = (AD \mod{n})$ is also a solution.

In fact, $(AD \pmod{n})$ is the least non-negative solution of the congruence.

The complete solution set is the set $[(AD \pmod{n})]$ = the equivalence class of $(AD \pmod{n})$ with respect to the equivalence relation "$\equiv (\mod{n})$".

The general method of solving such congruences is explained in detail at the end of this handout. We first illustrate this method by presenting two examples of its application.

Example 1: Consider the congruence $99 \cdot x \equiv 5 \pmod{13}$.

Here, $B = 99$ and $n = 13$ and $\gcd(99, 13) = 1$, and so, 99 has a $(\mod{13})$-inverse.

$A = 31$ is a $(\mod{13})$-inverse of $B = 99$.

[To see this, note that $A \cdot B = (31)(99) = 3,069$ and that $13 \mid (3,069 - 1) = 3,068 = (13)(256)$.

Thus, $(31)(99) \equiv 1 \pmod{13}$.

Since 31 is a $(\mod{13})$-inverse of 99, we multiply both sides of the original congruence by 31:

$(31)[99 \cdot x] \equiv (31)(5) \pmod{13}$, by Theorem 8.4.3, since $31 \equiv 31 \pmod{13}$ and $99 \cdot x \equiv 5 \pmod{13}$.

$[(31)(99)] \cdot x \equiv (31)(5) \pmod{13}$

Also, $[(31)(99)] \cdot x \equiv 1 \cdot x \pmod{13}$, by Theorem 8.4.3, since $[(31)(99)] \equiv 1 \pmod{13}$ and $x \equiv x \pmod{13}$, that is,

$\therefore x \equiv [(31)(99)] \cdot x \pmod{13}$ and $[(31)(99)] \cdot x \equiv (31)(5) \pmod{13}$.

$\therefore x \equiv (31)(5) \pmod{13}$, by transitivity.

$x \equiv 155 \pmod{13}$. Thus, $x = 155$ is a solution and any integer that is $(\mod{13})$-congruent to 155 is also a solution.

$\therefore x = (155 \pmod{13}) = 12$ is the least non-negative solution.

The solution set of the congruence $99 \cdot x \equiv 5 \pmod{13}$ is

$[12] = \{ \ldots, -27, -14, -1, 12, 25, 38, \ldots \}$.
Example 2: Solve the congruence

\[ 125x \equiv 47 \pmod{216}, \]

and determine the least non-negative solution.

Solution: We need to find a \((\mod 216)\) inverse of 125.

\[
\begin{align*}
125/216 & \equiv 1 \\
-125 & \equiv 91 \\
91/125 & \equiv 1 \\
-91 & \equiv -34 \\
34/91 & \equiv 2 \\
-68 & \equiv -23 \\
23/34 & \equiv 1 \\
-23 & \equiv 11 \\
11/23 & \equiv 2 \\
-2 & \equiv 1 \\
1/11 & \equiv 11 \\
-11 & \equiv 0
\end{align*}
\]

The gcd \((125, 216) = 1\), so there exist \((\mod 216)\) inverses of 125.

\[
\begin{align*}
91 & = (1)(216) - 1(125) \\
34 & = (1)(125) - (1)(91) \\
23 & = (1)(91) - (2)(34) \\
11 & = (1)(34) - (1)(23) \\
1 & = (1)(23) - (2)(11)
\end{align*}
\]

\[
\begin{align*}
1 & = (1)(23) - (2)[(1)(34) - (1)(23)] = (3)(23) - (2)(34) \\
1 & = (3)[(1)(91) - (2)(34)] - (2)(34) = (3)(91) - 8(34) \\
1 & = (3)(91) - (8)[(1)(125) - (1)(91)] = (1)(91) - 8(125) \\
1 & = (11)[(1)(216) - (1)(125)] - (8)(125) = (11)(216) - (19)(125) \\
1 & = (11)(216) + (-19)(125). \quad \text{So,} \ (-19) \text{ is a} \ (\mod 216) \text{ inverse of} \ 125.
\end{align*}
\]
To see this, consider how \( 1 - (-19)(125) = (113)(216) \), so \( 1 \equiv (-19)(125) \pmod{216} \).

We could proceed using \((-19)\) as the \((\pmod{216})\) inverse of 125, but it might be easier to use a positive \((\pmod{216})\)-inverse. Any integer which is \((\pmod{216})\)-congruent to \((-19)\) will do. We will use \( A = 197 = (-19 + 216) \).

With \( B = 125 \), \( AB = (197)(125) = 24,625 \) and \((24,625 - 1) = 24,624 = (114)(216) \).

So, \( 216 | (197)(125) - 1 \). Thus \( (197)(125) \equiv 1 \pmod{216} \).

The original congruence is \( 125x \equiv 47 \pmod{216} \).

Since \( (197)(125) \equiv 1 \pmod{216} \), \( [(197)(125)]x \equiv 1 \cdot x \pmod{216} \).

\[ \implies x \equiv [(197)(125)]x \pmod{216} \]

Also, since \( 125x \equiv 47 \pmod{216} \), \( (197)[125x] \equiv (197)(47) \pmod{216} \).

\[ \implies [(197)(125)]x \equiv (197)(47) \pmod{216} \]

\[ \implies x \equiv (197)(47) \pmod{216} \] by transitivity.

Since \( (197)(47) = 9,259 \), \( x \equiv 9,259 \pmod{216} \).

\[ \implies x = 9,259 \] is one solution.

\[ \implies x = (9,259 \pmod{216}) = 187 \] is the least non-negative solution.

The solution set is \( [187] = \{ \ldots , -245 , -29 , 187 , 403 , 619 , \ldots \} \).
The General Description of this Method for solving the Congruence

\[ B x \equiv D \pmod{n}, \text{ when } \gcd(B, n) = 1 \]

Since the \( \gcd(B, n) = 1 \), we can find a \((\mod{n})\)-inverse of \(B\), say \(A\), such that \(AB \equiv 1 \pmod{n}\).

Thus, \(A(Bx) \equiv AD \pmod{n}\), by Theorem 8.4.3, since \(A \equiv A \pmod{n}\) and \(Bx \equiv D \pmod{n}\), that is, \((AB)x \equiv AD \pmod{n}\).

Now, \(AB \equiv 1 \pmod{n}\) and \(x \equiv x \pmod{n}\). Therefore, \((AB)x \equiv 1 \cdot x \pmod{n}\), by Theorem 8.4.3, that is, \(x \equiv (AB)x \pmod{n}\).

Since \(x \equiv (AB)x \pmod{n}\) and \((AB)x \equiv AD \pmod{n}\), it follows that \(x \equiv AD \pmod{n}\), by transitivity.

Therefore, \(x\) is a solution of the congruence \(Bx \equiv D \pmod{n}\) if and only if \(x \equiv AD \pmod{n}\).

Thus, \(x = AD\) is one particular solution. By Theorem (NIB) 4, \(AD \equiv (AD \pmod{n}) \pmod{n}\), so \(x = (AD \pmod{n})\) is also a solution.

In fact, \((AD \pmod{n})\) is the least non-negative solution of the congruence.

The complete solution set is the set \([AD \pmod{n}] = \text{ the equivalence class of } (AD \pmod{n}) \text{ with respect to the equivalence relation } "\equiv (\pmod{n})"\).