Prove that the congruence $ax = b \pmod{n}$ has a solution if and only if $d = (a, n)$ divides $b$. If $d | b$, prove that the congruence has exactly $d$ incongruent solutions modulo $n$.

**Proof:**

**a)** Suppose $ax = b \pmod{n}$ has a solution $\Rightarrow$

$$ax - b = n \cdot q$$

where $q \in \mathbb{Z}$

Take $d = (a, n)$. We have

$$(1) \begin{cases} d = a \cdot t + n \cdot r \\ t, r \in \mathbb{Z} \end{cases}$$

Since $d = (a, n) \Rightarrow d | a$ and $d | n$ $\Rightarrow$

$$a = d \cdot q_1, \quad q_1, q_2 \in \mathbb{Z}$$

$$n = d \cdot q_2$$

Lastly from (1) it follows that

$$b = a \cdot x - n \cdot q = (d \cdot q_1) \cdot x - (d \cdot q_2) \cdot q$$

$$= d \left( q_1 x - q_2 \cdot q \right) = d \cdot c \Rightarrow$$

$d | b$, $d$ is a divisor of $b$.

**b)** Suppose $d = (a, n)$ and $d | b$.

Then we have

$$(2) \begin{cases} d = a \cdot t + n \cdot r \\ t, r \in \mathbb{Z} \end{cases}$$

From (2) it follows that

$$b = d \cdot c = (a \cdot t + n \cdot r) \cdot c = atc + nrc \Rightarrow$$

$$b - a \cdot (tc) = n \cdot (rc) \Rightarrow$$

$$a \cdot (tc) = b \pmod{n} \Rightarrow$$
a \ x = b \ (\text{mod} \ n) \text{ has a solution } x = (t \cdot c).

c) Suppose d \mid b (b = d \cdot q_3). \text{ Here } d = (a,n) \text{ and }

(3) \ a \ x = b \ (\text{mod} \ n).
\text{ If } d = (a,n) \text{ then we have: } a = d \cdot q_1, q_1, q_2 \in \mathbb{I} \quad n = d \cdot q_2

From (3) it follows that

(4) \ ax - b = n \cdot q, \quad q \in \mathbb{I} \\
\text{ Substituting } a, b \text{ and } n \text{ expressed in terms of } d \text{ we obtain } \ ax - b = n \cdot q \Rightarrow

(5) \ d \cdot q_1 \cdot x - d \cdot q_3 = d \cdot q_2 \cdot q

Let us divide (5) by d resulting in the following equation
\qquad q_1 \ x - q_3 = q_2 \cdot q
\quad \text{ or }

(6) \ q_1 \ x = q_3 \ (\text{mod} \ q_2) \\
\text{ Here } 1 = (q_1, q_2) \ (\text{Since } d = (a,n)) \\
\text{ Therefore solution of (6) can be found using Euclidean Algorithm (see p. 59).}

Lastly we obtain solutions of (6) which are also solutions of (3) in the form of equivalence class \([x]\) by modulo \(q_2\) meaning.

(7) \ [x] = \{x, x \pm q_2, x \pm 2q_2, \ldots, x \pm (d-1)q_2\}
\text{ But we know that } d \cdot q_2 = n. \text{ Therefore in (7) there are only } d \text{ different elements by modulo } n \\
\quad \{x, x + q_2, x + 2q_2, \ldots, x + (d-1)q_2\}
Example
#27
p. 61

\[ 8 \cdot x = 66 \pmod{78} \]

1) \[ d = (a,n) = (8, 78) = 2 \]

2) Dividing expression

\[ (*) \quad 8 \cdot x - 66 = 78 \cdot q \]
by \( d = 2 \) we get equivalent equation

\[ (**) \quad 4 \cdot x = 33 \pmod{39} \]
\[ (4 \cdot x - 33 = 39 \cdot q) \]

3) Now we can use Euclidian Alg. as follows

\[ 39 = 4 \cdot 9 + 3 \]
\[ 4 = 3 \cdot 1 + 1 \quad \Rightarrow \quad 1 = 4 - 3 \cdot 1 \]

\[ 3 = 3 \cdot 1 \]

Substituting (1) into (2) one obtains

\[ (3) \quad 1 = 4 - (39 - 4 \cdot 9 \cdot 1) = 4 \cdot 10 - 39 \]

Multiplying (3) by 33 we get that

\[ 33 = 4 \cdot 330 - 39 \cdot 33 \]

or

\[ 4 \cdot (330) - 33 = 39 \cdot 33 \quad \Rightarrow \]

\[ 4 \cdot (330) = 33 \pmod{39} \]

Lastly solution of (**) has the form
\[ x = [330] \quad \text{by modulo 39.} \]

There are only 2 different elements from \([330]\) by moduls 78:
\[ 330 \text{ and } 330 + 39 = 369 \quad (330 + 2 \cdot 39 = 330 + 78 = 330 \pmod{78}) \]
Thus solutions of (*) can be described as follows
1. \( x_1 = 330 \pmod{78} = 18 \)

2. \( x_2 = 330 + 39 = 369 \pmod{78} = 57 \)

P.62
#39
Suppose \((m,n) = 1\), and let \(a, b \in \mathbb{Z}\).
Prove that there exists an integer
\( x \) s.t. \( x \equiv a \pmod{m} \)
\( x \equiv b \pmod{n} \).

**Proof**

\((m,n) = 1\) means that \(m \cdot t + n \cdot r = 1\), \(t, r \in \mathbb{Z}\).
Now consider the following system
\[
\begin{cases}
  x \equiv a \pmod{m} \\
  x \equiv b \pmod{n}
\end{cases}
\]
or
\[
\begin{cases}
  x - a = m \cdot q_1, q_1, q_2 \in \mathbb{Z} \\
  x - b = n \cdot q_2
\end{cases}
\]
Subtracting second equation from the first we obtain
\[
(b - a) = m \cdot q_1 + n \cdot (-q_2)
\]
We know that there exist such \( t, r \) that
\[
1 = m \cdot t + n \cdot r
\]
Multiply (2) by \((b - a)\):
\[
(b - a) = m \cdot (t \cdot (b - a)) + n \cdot (r \cdot (b - a))
\]
Comparing with (2) we get that
\[
q_1 = t \cdot (b - a) \quad \text{and} \quad q_2 = r \cdot (b - a)
\]
Solution of the system (1) can be represented as follows:
\[
x = a + m \cdot [t \cdot (b-a)] = b + n \cdot [r \cdot (b-a)]
\]
On the other hand if we multiply equations (1) by \(q_2t\) and 
\(q_1r\) respectively and then sum them up we get
\[
x(q_2t + q_1t) - (aq_2 + bq_1r) = q_1q_2
\]
Therefore our \(x\) satisfies this equation and we should consider \([x]\) modulo \((q_1 \cdot q_2)\) as a solution.

**Example**

p. 62

#41

a) \((4)\)
\[
x - 2 = 5 \cdot q_1 \\
x - 3 = 8 \cdot q_2
\]
and \((5, 8) = 1\)

Use Euclidian alg. to obtain

\[
(5) \quad 1 = 5 \cdot (-3) + 8 \cdot (2)
\]

On the other hand substracting second equation of \((4)\) from the first we obtain

\[
(6) \quad \begin{align*}
1 &= 5 \cdot q_1 - 8 \cdot q_2 \\
&= 5 \cdot q_1 + 8 \cdot (-q_2)
\end{align*}
\]

Comparing \((6)\) with \((5)\) we get that

\[
(7) \quad q_1 = -3, \quad q_2 = -2
\]
and solution of \((4)\) has the form
\[
x = 2 + 5 \cdot q_1 = 3 + 8 \cdot q_2 = -13 = 27 \quad [40]
\]