p. 61 #26

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

<u>Proof:</u>

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

$$ax - b = n \cdot q \ , \ q \in \mathbb{Z}$$

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

(1)

$$\left\{ d = a \cdot t + n \cdot r \quad , \ t, r \in \mathbb{Z} \right.$$

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

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

Lastly from (1) it follows that

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

$d \mid b$, d is a divisor of b.

b) Suppose $d = (a,n)$ and $d \mid b$.

Then we have

(2)

$c \in \mathbb{Z}$ $$\left\{ d = a \cdot t + n \cdot r, \quad t, r \in \mathbb{Z} \right.$$

From (2) it follows that

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

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

$a \cdot (tc) = b \pmod{n} \Rightarrow$

$a\,x = b \pmod n$ has a solution
$x = (t \cdot c)$.

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

(3) $a\,x = b \pmod n$.

If $d = (a,n)$ then we have : $a = d \cdot q_1$, $q_1, q_2 \in \mathbb{Z}$
$n = d \cdot q_2$

From (3) it follows that

(4) $ax - b = n \cdot q, \quad q \in \mathbb{Z}$

Substituting a, b and n expressed in terms of d 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

$q_1\, x - q_3 = q_2 \cdot q$

or

(6) $q_1\, x \equiv q_3 \pmod{q_2}$

Here $1 = (q_1 , q_2)$ (Since $d = (a,n)$)

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) $[x] = \{x, x \pm q_2 , x \pm 2\,q_2 , . . , x \pm (d-1)\, q_2 \}$

But we know that $d \cdot q_2 = n$. Therefore in (7) there are only d different elements by modulo n

$\{x , x + q_2 , x + 2q_2 ,\ldots, x + (d-1)\, q_2\}$

Example

#27

p. 61

$8 \cdot x = 66 \pmod{78}$

1) $d = (a,n) = (8, 78) = 2$

2) Dividing expression

(*) $8 \cdot x - 66 = 78 \cdot q$

by $d = 2$ we get equivalent equation

(**) $4 \cdot x = 33 \pmod{39}$

$(4 \cdot x - 33 = 39 \cdot q)$

3) Now we can use Euchlidian Alg. as follows

$$
\begin{array}{l|l}
39 = 4 \cdot 9 + 3 & \\
4 = 3 \cdot 1 + 1 & \Rightarrow \\
\hline
3 = 3 \cdot 1 &
\end{array}
\qquad
\begin{array}{ll}
3 = 39 - 4 \cdot 9 & (1) \\
1 = 4 - 3 \cdot 1 & (2)
\end{array}
$$

Substituting (1) into (2) one obtains

(3) $1 = 4 - (39 - 4 \cdot 9 \cdot 1 = 4 \cdot 10 - 39$

Multiplying (3) by 33 we get that

$33 = 4 \cdot 330 - 39 \cdot 33$

or

$4 \cdot (330) - 33 = 39 \cdot 33 \Rightarrow$

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

Lastly solution of (**) has the form

$x = [330]$ by modulo 39.

There are only 2 different elements from [330] by moduls 78:
330 and 330 + 39 = 369 $(330 + 2 \cdot 39 = 330 + 78 \equiv 330 \pmod{78})$

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 $a, b \in$ Ì.

Prove that there exists an integer

x s.t. $x \equiv a \pmod{m}$

$x \equiv b \pmod{n}$.

<u>Proof</u>

$(m,n) = 1$ means that $m \cdot t + n \cdot r = 1$, t , $r \in$ Ì.

Now consider the following system

(1) $\begin{cases} x \int a \pmod{m} \\ x \int b \pmod{n} \end{cases}$ or

$\begin{cases} x - a = m \,.\, q_1 & , q_1, q_2 \text{ □Ì} \\ \end{cases}$

Substracting second equation from the first we obtain

(2) $b - a = m \cdot q_1 + n \cdot (-q_2)$

We know that there exist such t, r that

(3) $1 = m \cdot t + n \cdot r$

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

$q_1 = t \cdot (b - a)$ and $q_2 = r \cdot (b - a)$

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 $(q_2 t)$ and $(q_1\ r)$ respectively and then sum them up we get

$$x\,(q_2 t + q_1 t) - (aq_2 + bq_1 r) = q_1 q_2$$

Therefore our x satisfies this equation and we should consider [x] modulo $(q_1 \cdot q_2)$ as a solution.

<u>Example</u>

p. 62

#41

a) (4) $\begin{array}{l} x - 2 = 5 \cdot q_1 \\ x - 3 = 8 \cdot q_2 \end{array}$ and $(5, 8) = 1$

Use Euclidian alg. to obtain

(5) $1 = 5 \cdot (-3) + 8 \cdot (2)$

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

(6) $1 = 5 \cdot q_1 - 8 \cdot q_2 = 5 \cdot q_1 + 8 \cdot (-q_2)$

Comparing (6) with (5) we get that

(7) $q_1 = -3 \quad , \; q_2 = -2$

and solution of (4) has the form

$$x = 2 + 5 \cdot q_1 = 3 + 8 \cdot q_2 = -13 = 27\ [40]$$