i.e., $x \equiv (-3+5i) \pmod{15}$, $i = 0, 1, 2$

5. Solve the congruence $72x \equiv 18 \pmod{42}$

Solution: Since gcd $(72, 42) = 6$ and 6 divides 18, the congruence

$$72x \equiv 18 \pmod{42} \quad \ldots (1)$$

has exactly six solutions.

We now find a solution of (1). To find a solution of (1), we may consider the following congruence and find a solution of it.

$$12x \equiv 3 \pmod{7} \quad \ldots (2)$$

Now gcd $(12, 7) = 1$ and $12 = 7.1 + 5$, $7 = 1.5 + 2$

and $5 = 2.2 + 1$

Hence $1 = 5 + 2(-2) = 5 + (7-5)(-2)$

$= 7(-2) + 5(3) = 7(-2) + (12 - 7.1)3$

$= 12.3 + 7(-5)$.

According $3 = 12.9 + 7(-15)$

Hence $12.9 \equiv 3 \pmod{7}$. So, we find $x_0 = 9$ is a solution of (2). Hence $x_0 = 9$ is a solution of (1). Therefore the six solutions of (1) are

$$x = \left(9 + \frac{42}{6} i\right) \pmod{42} \quad i = 0, 1, 2, 3, 4, 5$$

i.e $x \equiv (9 + 7i) \pmod{42}$ $i = 0, 1, 2, 3, 4, 5$

## System of linear congruences

Let us consider the linear congruences

$$a_i x \equiv b_i \pmod{m_i} \quad i = 1, 2, \cdots, r$$

and let us enquire if it is possible to have a simultaneous solution of these congruences. In that case each individual congruence must have a solution.

Let $\gcd(a_i, m_i) = d_i \quad i = 1, 2, \cdots, r$

Then $d_i$ must be a divisor of $b_i$, $i = 1, 2, \cdots, r$.

Cancelling $d_i$ from the $i$th equation, the system reduces to

$$a_i' x \equiv b_i' \pmod{m_i'} \quad i = 1, 2, \cdots, r.$$

where $d_i a_i' = a_i$, $d_i b_i' = b_i$, $d_i m_i' = m_i$, $i = 1, 2, \cdots, r$

and $\gcd(a_i', m_i') = 1$, $i = 1, 2, \cdots r$

Each individual congruence has a unique solution of the form $x_i \equiv c_i \pmod{m_i}$ $i = 1, 2, \cdots r$

Then the problem is reduced to one of finding a common solution of

$$x \equiv c_i \pmod{m_i} \quad i = 1, 2, \cdots, r$$

The kind of problems that can be reduced to a system of linear congruences was in found in Chinese literature as early as first century AD. In later periods such problems were also found

in other countries. Because of their antiquity, this type of problem goes by the name of "Chinese Remainder theorem".

The method of congruence that is used to state the problem and to make the proof in a concise form was unknown to the ancients.

~~2.5.7~~ Theorem 2.5.7 (Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_r$ be positive integers such that $\gcd(m_i, m_j) = 1$ for $i \neq j$ and $c_1, c_2, \ldots, c_r$ be any integers. Then the system of linear congruences

$$x \equiv c_1 \pmod{m_1},\ x \equiv c_2 \pmod{m_2},\ \ldots,\ x \equiv c_r \pmod{m_r}$$

has a simultaneous solution which is unique modulo $m_1 m_2 \ldots m_r$ [i.e., if $x_0$ be a solution then $x_0 + k(m_1 m_2 \ldots m_r)$ is also a solution, where $k$ is an integer]

Proof: Let $m = m_1 m_2 \ldots m_r$ Let $M_k = \frac{m}{m_k}$ $k = 1, 2, \ldots, r$

Then $\gcd(M_k, m_k) = 1$ for $k = 1, 2, \ldots, r$

This implies that the linear congruence $M_k x \equiv 1 \pmod{m_k}$ has a unique solution modulo $m_k$. Let $x_k$ be the solution.

Then $M_k x_k \equiv 1 \pmod{m_k}$ and clearly $M_k x_k \equiv 0 \pmod{m_j}$ for $j \neq k$

Therefore $c_k M_k x_k \equiv c_k \pmod{m_k}$ and $c_k M_k x_k \equiv 0 \pmod{m_j}$ for $j \neq k$

Let us consider the integer

$$x_0 = c_1 M_1 x_1 + c_2 M_2 x_2 + \cdots + c_r M_r x_r$$

~~So, $x_0 \equiv c_1 \pmod{m_1}$, since $c_1 M_1 x_1 \equiv c_1 \pmod{m_1}$ and $c_k M_k x_k \equiv 0 \pmod{m_i}$ for $i \neq k$~~

So, $x_0 \equiv c_1 \pmod{m_1}$ since $c_1 M_1 x_1 \equiv c_1 \pmod{m_1}$ and $c_i M_i x_i \equiv 0 \pmod{m_1}$ for $i \neq 1$

Similarly $x_0 \equiv c_2 \pmod{m_2}$ since $c_2 M_2 x_2 \equiv c_2 \pmod{m_2}$ and $c_i M_i x_i \equiv 0 \pmod{m_2}$ for $i \neq 2$

- - -

Similarly, $x_0 \equiv c_r \pmod{m_r}$ since $c_r M_r x_r \equiv c_r \pmod{m_r}$ .. and $c_i M_i x_i \equiv 0 \pmod{m_r}$ if $r$

This shows that $x_0$ is a solution of the given system of congruences.

Let $x'$ be any solution of the given system of congruences

Then $x' \equiv c_k \pmod{m_k}$ for $k = 1, 2, \ldots, r$

$x' \equiv c_k \pmod{m_k}$ and $x_0 \equiv c_k \pmod{m_k}$

$\Rightarrow x' \equiv x_0 \pmod{m_k}$ for $k = 1, 2, \ldots r$

Consequently, $x' \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$

[using the theorem that $x \equiv y \pmod{m_i}$, for $i = 1, 2, \ldots r$

$\Leftrightarrow$ (equivalent to) $x \equiv y \pmod{m}$ where

$m$ is the l.c.m (least common multiple) of $m_1, m_2, \ldots m_r$]

Note This shows that the solution is unique modulo $m_1 m_2 \cdots m_r$

Note: Let $a_1, a_2, \ldots, a_n$ be integers different from 0