

# Abstract Algebra by Pinter, Chapter 23, question B3

Amir Taaki

Chapter 23 on Number Theory

## Contents

<b>Proof</b>	<b>1</b>
Initial Question . . . . .	1
Simultaneous Solution for Three Elements . . . . .	1
Generalizing to $k + 1$ through induction . . . . .	3
Relation between gcd and lcm operators . . . . .	3
Proving equivalency holds under gcd for $k + 1$ . . . . .	3
Generalizing lcm to Multiple Arguments . . . . .	3
Solution $c \equiv c_i$ is also a Solution in the lcm of the gcds . . . . .	4
There is a Common Solution for $c$ and $c_{k+1}$ . . . . .	4

## Proof

### Initial Question

We are given  $k$  congruences

$$x \equiv c_1 \pmod{m_1} \quad x \equiv c_2 \pmod{m_2} \quad \dots \quad x \equiv c_k \pmod{m_k}$$

for all  $i, j \in \{1, \dots, k\}$

$$c_i \equiv c_j \pmod{d_{ij}}$$

where  $d_{ij} = \gcd(m_i, m_j)$ .

Prove there is an  $x$  satisfying all  $k$  congruences simultaneously, and the solution is of the form

$$x \equiv c \pmod{t}$$

where  $t = \text{lcm}(m_1, m_2, \dots, m_k)$ .

### Simultaneous Solution for Three Elements

We will proceed to prove these statements through induction, first starting with the case of proving there is a simultaneous solution for  $c_1, c_2$  and  $c_3$ .

It has been shown earlier in theorem 3 that there is a solution for two equations  $x \equiv a \pmod{n}$  and  $x \equiv b \pmod{m}$ , only exists if

$$a \equiv b \pmod{d}$$

$$d = \gcd(m, n)$$

For the first two equations, there is therefore a simultaneous solution because

$$c_1 \equiv c_2 \pmod{d_{12}}$$

Earlier in theorem 4, it was shown that if  $x \equiv a \pmod{n}$  and  $x \equiv b \pmod{m}$  have a simultaneous solution, it is of the form

$$x \equiv c \pmod{t}$$

$$t = \text{lcm}(m, n)$$

So therefore the solution of  $x \equiv c_1 \pmod{m_1}$  and  $x \equiv c_2 \pmod{m_2}$  is

$$x \equiv c \pmod{t}$$

$$t = \text{lcm}(m_1, m_2)$$

We want to know if there is a solution  $x$  for  $x = c \pmod{t}$  and  $x = c_3 \pmod{m_3}$ . That is whether the statement

$$c_3 \equiv c \pmod{\text{gcd}(t, m_3)}$$

is true.

But we know that  $\text{gcd}(a, \text{lcm}(b, c)) = \text{lcm}(\text{gcd}(a, b), \text{gcd}(a, c))$  so

$$\begin{aligned} \text{gcd}(t = \text{lcm}(m_1, m_2), m_3) &= \text{lcm}(\text{gcd}(m_1, m_3), \text{gcd}(m_2, m_3)) \\ &= \text{lcm}(d_{13}, d_{23}) \end{aligned}$$

So we want to know whether this statement is true

$$\begin{aligned} c_3 &\equiv c \pmod{\text{gcd}(t, m_3)} \\ &\equiv c \pmod{\text{lcm}(d_{13}, d_{23})} \end{aligned}$$

At the start it was stated that  $c_3 \equiv c_1 \pmod{d_{13}}$ , and we also we know that

$$\begin{aligned} c \equiv c_1 \pmod{m_1} &\implies c \equiv c_1 \pmod{d_{13}} \\ \therefore c &\equiv c_3 \pmod{d_{13}} \end{aligned}$$

Likewise  $c_3 \equiv c_2 \pmod{d_{23}} \implies c \equiv c_3 \pmod{d_{23}}$

Now from the last part of theorem 4, we note that

$$m \mid (x - c) \text{ and } n \mid (x - c) \iff t \mid (x - c)$$

or

$$x \equiv c \pmod{m} \text{ and } x \equiv c \pmod{n} \iff x \equiv c \pmod{t}$$

Note that

$$d_{13} \mid (c - c_3) \text{ and } d_{23} \mid (c - c_3) \iff \text{lcm}(d_{13}, d_{23}) \mid (c - c_3)$$

or

$$c \equiv c_3 \pmod{d_{13}} \text{ and } c \equiv c_3 \pmod{d_{23}} \iff c \equiv c_3 \pmod{\text{lcm}(d_{13}, d_{23})}$$

That is we can state that

$$c_3 \equiv c \pmod{\text{lcm}(d_{13}, d_{23})}$$

But  $\text{lcm}(d_{13}, d_{23}) = \text{gcd}(t, m_3)$ . So by theorem 3 because

$$c_3 \equiv c \pmod{\text{gcd}(t, m_3)}$$

there is a simultaneous solution of

$$\begin{aligned} x &\equiv c \pmod{t} \\ x &\equiv c_3 \pmod{m_3} \end{aligned}$$

And this is also the solution for

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

## Generalizing to $k + 1$ through induction

Now we will generalize this using induction on  $k+1 \in \mathbb{Z}$  terms where we assume  $S_k$  is true, proving the statement  $S_{k+1}$  is true, and therefore it is true for all integers.

Assume there is a solution of  $k$  congruences

$$x \equiv c_1 \pmod{m_1} \quad \dots \quad x \equiv c_k \pmod{m_k}$$

of the form

$$\begin{aligned} x &\equiv c \pmod{t} \\ t &= \text{lcm}(m_1, \dots, m_k) \end{aligned}$$

Note that  $\forall i, j \in \{1, \dots, k\}$

$$\begin{aligned} c_i &\equiv c_j \pmod{d_{ij}} \\ d_{ij} &= \gcd(m_i, m_j) \end{aligned}$$

that is

$$c_{k+1} = c_i \pmod{d_{k+1,i}}$$

We want to know if there is an  $x \pmod{t'}$  which is the solution for  $x \equiv c \pmod{t}$  and  $x \equiv c_{k+1} \pmod{m_{k+1}}$ . That is whether the statement

$$c_{k+1} \equiv c \pmod{\gcd(t, m_{k+1})}$$

is true or not.

## Relation between gcd and lcm operators

From chapter 22, exercise H4, let  $a \star b = \gcd(a, b)$  and  $a \circ b = \text{lcm}(a, b)$  then it is trivial to show that

$$a \star (b \circ c) = (a \star b) \circ (a \star c)$$

and we know that the lcm operation is associative.

$$m_1 \circ m_2 \circ \dots \circ m_k = m_1 \circ (m_2 \circ (\dots \circ m_k))$$

so

$$\begin{aligned} m_{k+1} \star (m_1 \circ m_2 \circ \dots \circ m_k) &= (m_{k+1} \star m_1) \circ (m_{k+1} \star (m_2 \circ \dots \circ m_k)) \\ &= (m_{k+1} \star m_1) \circ (m_{k+1} \star m_2) \circ (m_{k+1} \star (m_3 \circ \dots \circ m_k)) \\ &= (m_{k+1} \star m_1) \circ \dots \circ (m_{k+1} \star m_k) \end{aligned}$$

That is

$$\gcd(\text{lcm}(m_1, \dots, m_k), m_{k+1}) = \text{lcm}(\gcd(m_1, m_{k+1}), \dots, \gcd(m_k, m_{k+1}))$$

## Proving equivalency holds under gcd for $k + 1$

At the beginning it was stated that  $\forall i \in \{1, \dots, k\}$

$$c_{k+1} \equiv c_i \pmod{d_{k+1,i}}$$

and we also know that

$$\begin{aligned} c &\equiv c_i \pmod{m_i} \\ c - c_i &= qm_i = q(s d_{k+1,i}) \\ \implies c &\equiv c_i \pmod{d_{k+1,i}} \end{aligned}$$

## Generalizing lcm to Multiple Arguments

The lcm is defined as if  $c = \text{lcm}(a, b)$  then

1.  $a \mid c$  and  $b \mid c$
2. For any  $x$  if  $a \mid x$  and  $b \mid x \implies c \mid x$

This can be generalized for any number of arguments in the lcm by noting that since  $c = \text{lcm}(x_1, x_2, \dots, x_n)$  then  $\forall i \in \{1, \dots, n\}$  then 1.  $x_i \mid c$  for 2., note that the common multiples of  $\{x_1, \dots, x_n\}$  form an ideal of  $\mathbb{Z}$  by  $\langle c \rangle = \langle x_1 \rangle \cap \dots \cap \langle x_n \rangle$ , and so every common multiple is a multiple of  $c$ .

$\therefore$  any  $v$  such that  $\forall x_i \in X : x_i \mid v \implies c \mid v$ .

## Solution $c \equiv c_i$ is also a Solution in the lcm of the gcds

From theorem 4, we generalize that

$$\begin{aligned} m_1 | x, \dots, m_n | x &\implies t | x \\ m_1 | (x - c), \dots, m_n | (x - c) &\implies t | (x - c) \\ x \equiv c \pmod{m_1} &\quad \dots \quad x \equiv c \pmod{m_n} \implies x \equiv c \pmod{t} \end{aligned}$$

where  $t = \text{lcm}(m_1, \dots, m_n)$

Now note that

$$d_{k+1,1} | (c - c_i) \quad \dots \quad d_{k+1,k} | (c - c_i) \implies \text{lcm}(d_{k+1,1}, \dots, d_{k+1,k}) | (c - c_i)$$

or

$$c \equiv c_i \pmod{d_{k+1,1}} \quad \dots \quad c \equiv c_i \pmod{d_{k+1,k}} \implies c \equiv c_i \pmod{\text{lcm}(d_{k+1,1}, \dots, d_{k+1,k})}$$

## There is a Common Solution for $c$ and $c_{k+1}$

So,

$$c \equiv c_i \pmod{\text{lcm}(\gcd(m_{k+1}, m_1), \dots, \gcd(m_{k+1}, m_k))}$$

But we know that

$$\begin{aligned} \text{lcm}(\gcd(m_{k+1}, m_1), \dots, \gcd(m_{k+1}, m_k)) &= \gcd(\text{lcm}(m_1, \dots, m_k), m_{k+1}) \\ &\implies c \equiv c_i \pmod{\gcd(t, m_{k+1})} \end{aligned}$$

where  $t = \text{lcm}(m_1, \dots, m_k)$

And because of this, by theorem 3, because  $\forall i \in \{1, \dots, k\}$ ,  $c \equiv c_i \pmod{\gcd(t, m_{k+1})}$ , there is an  $x$  such that

$$\begin{aligned} x &\equiv c \pmod{t} \\ x &\equiv c_{k+1} \pmod{m_{k+1}} \end{aligned}$$

which because  $x \equiv c \pmod{t}$ , this is also the solution for

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\dots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

Furthermore this solution takes the form

$$\begin{aligned} x &\equiv c' \pmod{\text{lcm}(t, m_{k+1})} \\ &\equiv c' \pmod{t'} \end{aligned}$$

where  $t' = \text{lcm}(m_1, m_2, \dots, m_k)$