Abstract Algebra by Pinter, Chapter 23, question B3

Amir Taaki

Abstract

Chapter 23 on Number Theory

Contents

1 Proof

1.1 Initial Question

We are given k congruences

$$x \equiv c_1 (\operatorname{mod} m_1) \qquad x \equiv c_2 (\operatorname{mod} m_2) \qquad \cdots \qquad x \equiv (\operatorname{mod} m_k)$$

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

$$c_i \equiv c_j (\operatorname{mod} d_{ij})$$

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

$$x \equiv c (\operatorname{mod} t)$$

where $t = \operatorname{lcm}(m_1, m_2, \ldots, m_k)$.

1.2 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 $x \equiv a (\operatorname{mod} n)$ and $x \equiv b (\operatorname{mod} m)$, only exists if

$$a \equiv b (\operatorname{mod} d)$$
$$d = \gcd(m, n)$$

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

$$c_1 \equiv c_2 (\operatorname{mod} d_{12})$$

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

$$x \equiv c (\operatorname{mod} t)$$
$$t = \operatorname{lcm}(m, n)$$

So therefore the solution of $x \equiv c_1 (\operatorname{mod} m_1)$ and $x \equiv c_2 (\operatorname{mod} m_2)$ is

$$x \equiv c (\operatorname{mod} t)$$

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

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

$$c_3 \equiv c[\operatorname{mod} \gcd(t, m_3)]$$

is true.

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

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

So we want to know whether this statement is true

$$\begin{aligned} c_3 &\equiv c[\operatorname{mod} \gcd(t, m_3)] \\ &\equiv c[\operatorname{lcm}(d_{13}, d_{23})] \end{aligned}$$

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

$$c \equiv c_1 (\operatorname{mod} m_1) \implies c \equiv c_1 (\operatorname{mod} d_{13})$$

$$\therefore c \equiv c_3 (\operatorname{mod} d_{13})$$

Likewise $c_3 \equiv c_2 (\operatorname{mod} d_{23}) \implies c \equiv c_3 (\operatorname{mod} d_{23})$

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

$$x \equiv c(\operatorname{mod} m) \text{ and } x \equiv c(\operatorname{mod} n) \iff x \equiv c(\operatorname{mod} t)$$

Note that

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

or

$$c \equiv c_3 (\operatorname{mod} d_{13}) \text{ and } c \equiv c_3 (\operatorname{mod} d_{23}) \iff c \equiv c_3 [\operatorname{mod} \operatorname{lcm}(d_{13}, d_{23})]$$

That is we can state that

$$c_3 \equiv c[\operatorname{mod} \operatorname{lcm}(d_{13}, d_{23})]$$

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

$$c_3 \equiv c[\operatorname{mod} \gcd(t, m_3)]$$

there is a simultaneous solution of

$$\begin{aligned} x &\equiv c(\operatorname{mod} t) \\ x &\equiv c_3 (\operatorname{mod} m_3) \end{aligned}$$

And this is also the solution for

$$\begin{aligned} x &\equiv c_1 (\operatorname{mod} m_1) \\ x &\equiv c_2 (\operatorname{mod} m_2) \end{aligned}$$

1.3 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

$$x \equiv c_1 (\operatorname{mod} m_1) \qquad \cdots \qquad x \equiv c_k (\operatorname{mod} m_k)$$

of the form

$$x \equiv c (\operatorname{mod} t)$$
$$t = \operatorname{lcm}(m_1, \ldots, m_k)$$

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

$$c_i \equiv c_j (\operatorname{mod} d_{ij})$$
$$d_{ij} = \gcd(m_i, m_j)$$

that is

$$c_{k+1} = c_i (\operatorname{mod} d_{k+1,i})$$

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

$$c_{k+1} \equiv c[\operatorname{mod} \gcd(t, m_{k+1})]$$

is true or not.

1.4 Relation between gcd and lcm operators

From chapter 22, exercise H4, let $a \star b = \gcd(a, b)$ and $a \circ b = \operatorname{lcm}(a, b)$ 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.

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

so

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

That is

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

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

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

$$c_{k+1} \equiv c_i (\operatorname{mod} d_{k+1,i})$$

and we also know that

$$c \equiv c_i (\operatorname{mod} m_i)$$
$$c - c_i = q m_i = q(s d_{k+1,i})$$
$$\implies c \equiv c_i (\operatorname{mod} d_{k+1,i})$$

1.6 Generalizing lcm to Multiple Arguments

The lcm is defined as if $c = \operatorname{lcm}(a, b)$ 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 $c = \operatorname{lcm}(x_1, x_2, \ldots, x_n)$ then $\forall i \in \{1, \ldots, n\}$ then 1. $x_i \mid c$ for 2., note that the common multiples of $\{x_1, \ldots, x_n\}$ form an ideal of $\mathbb{Z}$ by $\langle c \rangle = \langle x \rangle \cap \cdots \cap \langle x_n \rangle$, and so every common multiple is a multiple of c.

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

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

From theorem 4, we generalize that

$$m_1 \mid x, \cdots, m_n \mid x \implies t \mid x$$

$$m_1 \mid (x-c), \cdots, m_n \mid (x-c) \implies t \mid (x-c)$$

$$x \equiv c (\bmod m_1) \qquad \cdots \qquad x \equiv c (\bmod m_n) \implies x \equiv c (\bmod t)$$

where $t = \operatorname{lcm}(m_1, \ldots, m_n)$

Now note that

$$d_{k+1,1} \mid (c - c_i) \qquad \cdots \qquad d_{k+1,k} \mid (c - c_i) \implies \operatorname{lcm}(d_{k+1,1}, \ldots, d_{k+1,k}) \mid (c - c_i)$$

or

$$c \equiv c_i (\bmod d_{k+1,1}) \qquad \cdots \qquad c \equiv c_i (\bmod d_{k+1,k}) \implies c \equiv c_i [\bmod \operatorname{lcm}(d_{k+1,1}, \ldots, d_{k+1,k})]$$

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

So,

$$c \equiv c_i [\bmod \operatorname{lcm}(\gcd(m_{k+1}, m_1), \ldots, \gcd(m_{k+1}, m_k))]$$

But we know that

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

$$\implies c \equiv c_i [\bmod \gcd(t, m_{k+1})]$$

where $t = \operatorname{lcm}(m_1, \ldots, m_k)$

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

$$x \equiv c (\bmod t)$$

$$x \equiv c_{k+1} (\bmod m_{k+1})$$

which because $x \equiv c (\bmod t)$, this is also the solution for

$$x \equiv c_1 (\bmod m_1)$$

$$\cdots$$

$$x \equiv c_k (\bmod m_k)$$

Furthermore this solution takes the form

$$\begin{aligned} x &\equiv c' [\bmod \operatorname{lcm}(t, m_{k+1})] \\ &\equiv c' (\bmod t') \end{aligned}$$

where $t' = \operatorname{lcm}(m_1, m_2, \ldots, m_k)$