A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 3EB

Bookmark

Show all steps: ON

Problem

Use Theorems 3 and 4 to prove the following: Suppose we are given k congruences

There is an x satisfying all k congruences simultaneously if for all $i, j \in \{1, \ldots, k\}$, $c_i \equiv c_j \pmod{d_{ij}}$, where $d_{ij} = \gcd(m_i, m_j)$. Moreover, the simultaneous solution is of the form $x \equiv c \pmod{t}$, where $t =$ 1cm $(m_1, m_2, \ldots, m_k)$.

Step-by-step solution

Step 1 of 4

Here, objective is to prove the given statement.

Number of congruence $= k$

Comment

Step 2 of 4

Theorem $3:$

Consider $x = a(\bmod n), x = b(\bmod m)$ there is an integer satisfying both congruence's simultaneously if and only if , $a = b(\bmod b), \gcd(m, n)$

Theorem $4:$

If a pair of congruence's $x = a(\bmod n), x = b(\bmod m)$ has a simultaneous solution, then the solution is of the form $x = c(\bmod t)$

Where t is the least common multiple of (m, n)

Comment

Step 3 of 4

Consider

$x = c_1(\bmod m_1), x = c_2(\bmod m_1), \ldots. x = c_k(\bmod m_k)$

Consider the first two equations $x = c_1(\bmod m_1), x = c_2(\bmod m_1),$

The solution is of the form $x = c(\bmod t)$

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

Comment

Step 4 of 4

Consider the first two congruence's simultaneously with

$x = c_3(\bmod m_3)$

$\gcd(t, m_3) = lcm(d_{13}, d_{23})$
$c_3 = c_1(\bmod d_{13})$
$c_3 = c_2(\bmod d_{23})$
$c_3 = c[\bmod \gcd(t, m_3)]$

Repeat the above process for *k* times

Then, $c_i = c_j[\bmod d_{ij}];$ where $d_{ij} = \gcd(m_i, m_j)], i, j \in \{1, 2 \ldots k\}$

The solution is of the form $x = c(\bmod t)$

Where, $t = \text{lcm}(m_1, m_2 \ldots. m_k)$

Hence, proved.

Comment