Integer Arithmetic

Gunjan.Rehani@bennett.edu.in, Madhushi.Verma@bennett.edu.in

CSE, SEAS
Bennett University

June 17, 2021

Overview

Linear Congruence

Inverses

Chinese Remainder Theorem

Linear Congruence

An expression of the form $ax \equiv b$ (mod m) where
$a \not\equiv 0$ (mod m) i.e m does not divide a, is called a linear congruence modulo m.
Solution Let d=gcd(a,m)
i) The linear congruence has a solution if and only if $d|b$ and there is no solution otherwise.
ii) The solution of the linear congruence can be obtained by solving the following congruence:
(a/d)x=(b/d) mod (m/d)
iii) The given congruence has d solutions which are mutually in congruent modulo m.
Note: Let x_0 be the unique smallest positive solution, then
x_0,$x_0 + (m/d)$,$x_0 + 2(m/d)$+...+$x_0 + (d-1)(m/d)$
will be the d solutions of the given congruence.

Examples

Find the solution of the congruence
$6x \equiv 3(mod 9)$
Solution:
gcd(6,9)=3 and 3 divides 3.
Thus 3 solutions are possible.
By step ii)
$2x \equiv 1(mod 3)$
Choosing x=0,1,2 and testing the congruence, we get $x_0 = 2$
We have m=9 and d=3
Thus the other two solution are
$x_1 = x_0 + (m/d) = 2+3 = 5$
$x_2 = x_0 + 2(m/d) = 2+6 = 8$
Hence 2,5 and 8 is the solution.

1. Find the solution of the congruence
$2x \equiv 1 (\text{mod } 5)$
2. Find the solution of the congruence
$3x \equiv 2 (\text{mod } 4)$
3. Find the solution of the congruence
$4x \equiv 3 (\text{mod } 2)$
4. Find the solution of the congruence
$234x \equiv 60 (\text{mod } 762)$

Definition of Congruence

Definition of Congruence:
If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides (a-b).
$a \equiv b \pmod{m}$
$a \not\equiv b \pmod{m}$

Inverses

A) Additive Inverse
In Z_n, two numbers a and b are additive inverses of each other if
$a + b \equiv 0 \pmod{n}$
Therefore, in Z_n, additive inverse of a can be calculated as b=n-a.
e.g. Additive inverse of 4 in Z_{10} is 10-4=6
Find all additive inverse pairs in Z_{10}
Solution: (0,0),(1,9),(2,8),(3,7),(4,6),(5,5)

B) Multiplicative Inverse

In Z_n, two numbers a and b are multiplicative inverses of each other if
$a \times b \equiv 1 \pmod{n}$

e.g. Multiplicative inverse of 3 is 7 in Z_{10}

Note: a has a multiplicative inverse in Z_n, if and only if
gcd(n,a)=1.

In this case,a and n are said to be relatively prime.

Try Yourself

1. Find the multiplicative inverse of 8 in Z_{10}
2. Find all the inverses in Z_{10}

Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime as shown below:

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$
... $x \equiv a_k \pmod{m_k}$

CRT states that the above equations have a unique solution if the moduli are relatively prime.

Steps

1. Find M= $m_1 \times m_2 \times m_3 ... \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1, M_2 = M/m_2, M_3 = M/m_3, ..., M_k = M/m_k$
3. Find the multiplicative inverses of $M_1, M_2, ...M_k$ using the corresponding moduli $(m_1, m_2, ...m_k.)$
Call the inverses M_1^-1,M_2^-1,...M_k^-1.
4. The solution to the simultaneous equations is
x=$(a_1 M_1 M_1^- 1 + a_2 M_2 M_2^- 1 + ... + a_k M_k M_k^- 1)$mod M

Find the solution to the simultaneous equations
$x \equiv 2 \text{ mod } 3$
$x \equiv 3 \text{ mod } 5$
$x \equiv 2 \text{ mod } 7$
So $a_1 = 2, a_2 = 3, a_3 = 2$
1. $m_1 = 3, m_2 = 5, m_3 = 7$
2. $M_1 = M/m_1 = 105/3 = 35$
$M_2 = M/m_2 = 105/5 = 21$
$M_3 = M/m_3 = 105/7 = 15$
3. $M_1^-1 : 35 \times () \equiv 1(mod3)$ The inverses are
$M_1^-1 = 2, M_2^-1 = 1, M_3^-1 = 1$ (use trial and error)
4. x=$(a_1 \times M_1 \times M_1^-1 + a_2 \times M_2 \times M_2^-1 + a_3 \times M_3 \times M_3^-1) modM$
=$(2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1)$ mod M
=(140+63+30) mod 105
=233 mod 105
=23

Find an integer that has a remainder of 3 when divided by 7 and 13 but is divisible by 12 using CRT.

Solution
$x \equiv 3 \bmod 7$
$x \equiv 3 \bmod 13$
$x \equiv 0 \bmod 12$
x=276