Congruences

Debdeep Mukhopadhyay

Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Congruences: Modular Arithmetic**
- **Chinese Remainder Theorem (CRT)**
  - **expressing the whole in parts**

Congruences

- We say that a is congruent to b modulo m, and we write $a \equiv b \bmod m$, if m divides b-a.
- Example: $-2 \equiv 19 \pmod{21}$, $20 \equiv 0 \pmod{10}$.
- Congruence modulo m is an equivalence relation on the integers.
  - any integer is congruent to itself modulo m (reflexivity)
  - $a \equiv b \bmod m$, implies that $b \equiv a \bmod m$ (symmetry)
  - $a \equiv b \bmod m$ and $b \equiv c \bmod m$ implies $a \equiv c \bmod m$ (transitivity)

The following are equivalent

- $a \equiv b \bmod m$
- There is $k \in Z$, with $a = b + km$
- When divided by m, both a and b leave the same remainder.
- Equivalence Class of ***a modulo m*** consists of all integers that are obtained by adding a with integral multiples of m
  - called residue class of ***a mod m***

Example

- **Residue class of 1 mod 4:**
  {1, 1±4, 1±2*4, 1±3*4,…}
- **The set of residue classes mod m is denoted by Z/mZ.**
  - **it has m elements, 0, 1, …, m-1**
  - **this is called a complete set of incongruent residues (complete system)**
  - **Examples for complete system for mod 5 is:**
    {0, 1, …, 4}, {-12, -15, 82, -1, 31} etc.

Theorem

- **a≡b mod m, and c≡d mod m, implies that -a≡-b mod m, a + c ≡ b + d mod, and ac ≡ bd mod m.**

Example

Prove that $2^{2^5}+1$ is divisible by 641.

Note that: $641 = 640 + 1 = 5*2^7 + 1$.

Thus, $5*2^7 \equiv -1 \bmod 641$.

$\Rightarrow (5*2^7)^4 \equiv (-1)^4 \bmod 641$

$\Rightarrow 5^4*2^{28} \equiv 1 \bmod 641$

$\Rightarrow (625 \bmod 641)*2^{28} \equiv 1 \bmod 641$

$\Rightarrow (-2^4)*2^{28} \equiv 1 \bmod 641$

$\Rightarrow 2^{32} \equiv -1 \bmod 641$

Theorems

If $a \equiv b (\bmod\ m)$, and k divides a, b, and m,

$$\frac{a}{k} \equiv \frac{b}{k} (\bmod\ \frac{m}{k})$$

Let, k divide both a and b and let $\gcd(k, m) = d$.

Then, $a \equiv b (\bmod\ m)$ implies, $\frac{a}{k} \equiv \frac{b}{k} (\bmod\ \frac{m}{d})$

Linear Congruences

- **Solving congruences modulo m is the same as solving equations in** Z_m.

$$\boxed{\text{If } ax \equiv b (\text{mod } m)}$$

- Here, a and b are integers.
- Is it solvable?
- How many solutions exist?

Theorem

Let, $d = \gcd(a, m)$. The congruence $ax \equiv b(\text{mod } m)$ is solvable for x iff $d \mid b$. If $d \mid b$, then all solutions are congruent to each other modulo m / d, *ie.* there is a unique solution modulo m / d.
In particular, if $\gcd(a, m) = 1$, then the congruence has a unique solution modulo m.

Example

$21x \equiv 9 \pmod{15}$ is solvable and has 3 solutions modulo 15.

$21x \equiv 8 \pmod{15}$ is not solvable.

The Chinese Remainder Theorem (CRT)

- **It solves a system of congruences.**
- **Suppose $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers.**
- **System of congruences:**

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

CRT asserts that there is a unique solution to this system

Example

- x≡3 mod 5
- x≡1 mod 3
- x≡ ? mod 15
- You can verify that the only answer is 13 mod 15. The first thing to explain why there is only one solution.

Uniqueness

- X(x)=(x mod 5, x mod 3)

$$
\begin{array}{rclrclrcl}
\chi(0) & = & (0,0) & \chi(1) & = & (1,1) & \chi(2) & = & (2,2) \\
\chi(3) & = & (3,0) & \chi(4) & = & (4,1) & \chi(5) & = & (0,2) \\
\chi(6) & = & (1,0) & \chi(7) & = & (2,1) & \chi(8) & = & (3,2) \\
\chi(9) & = & (4,0) & \chi(10) & = & (0,1) & \chi(11) & = & (1,2) \\
\chi(12) & = & (2,0) & \chi(13) & = & (3,1) & \chi(14) & = & (4,2).
\end{array}
$$

Note that the mapping is bijective…

Example

- $M=5 \times 3=15$
- $M_1=15/5=3$, $3^{-1} \bmod 5=2$
- $M_2=15/3=5$, $5^{-1} \bmod 3=2$
- $x=(3 \times 3 \times 2+1 \times 5 \times 2) \bmod 15$
  $=28 \bmod 15=13$

What is the principle?

Generalization

- We shall present a constructive proof
- In fact, CRT gives an explicit formula for $X^{-1} \bmod M$, where $M=m_1 m_2 \ldots m_r$
- Compute, $M_i=M/m_i$, for $1 \le i \le r$
  - Thus, $\gcd(m_i, M_i)=1$
- Compute $y_i=M_i^{-1} \bmod m_i$

- Thus, $M_i y_i \equiv 1 \pmod{m_i}$, for $1 \le i \le r$
- Define,

$$\rho(a_1, \ldots, a_r) = \sum_{i=1}^{r} a_i M_i y_i \bmod M.$$

- Compute, $\rho \bmod m_i \equiv a_i$ [This is because $M_i y_i \equiv 1 \pmod{m_i}$ and $M_i y_i \equiv 0 \pmod{m_j}$]
- Since, the domain and range have the same cardinality and the function X() is onto, by our previous discussion the function is bijective. Thus the solution is unique modulo M.

The CRT Theorem

(Chinese remainder theorem) *Suppose $m_1, \ldots, m_r$ are pairwise relatively prime positive integers, and suppose $a_1, \ldots, a_r$ are integers. Then the system of r congruences $x \equiv a_i \pmod{m_i}$ $(1 \le i \le r)$ has a unique solution modulo $M = m_1 \times \cdots \times m_r$, which is given by*

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \bmod m_i$, for $1 \le i \le r$.

Example

Suppose, $x \leq 1000$.

Solve,

$$x \equiv 5 \pmod{7}$$

$$x \equiv 3 \pmod{11}$$

$$x \equiv 2 \pmod{13}$$