e-PGPathshala

Subject : Computer Science

Paper: Cryptography and Network Security

Module: Chinese Remainder Theorem

Module No: CS/CNS/11

Quadrant 1 – e-text

Cryptography and Network Security

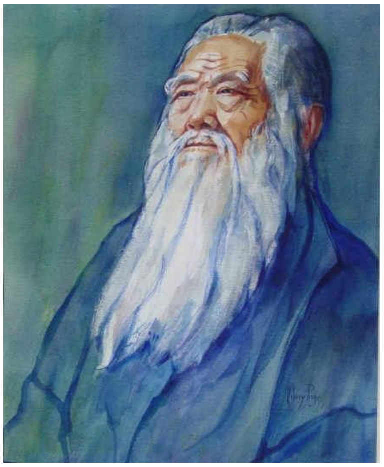
Module 11- Chinese Remainder Theorem

Learning Objectives

- To introduce prime numbers and their applications in cryptography.
- To discuss about Euler’s and Fermat’s Theorem.
- To discuss various examples Euler’s and Fermat’s Theorem.
- To describe the Chinese remainder theorem and its application.

10.1. Chinese Remainder Theorem

This theorem has this name because it is a theorem about *remainders* and was first discovered in the 3rd century AD by the Chinese mathematician Sunzi in *Sunzi Suanjing*.



The **Chinese remainder theorem** is a theorem of number theory, which states that, if one knows the remainders of the division of an integer *n* by several integers, then one can determine uniquely the remainder of the division of *n* by the product of these integers, under the condition that the divisors are pairwise coprime.

The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers.

10.2. Theorem Statement

Let $n_1, ..., n_k$ be integers greater than 1, which are often called *moduli* or *divisors*. Let us denote by N the product of the n_i.

The Chinese remainder theorem asserts that if the n_i are pairwise coprime, and if $a_1, ..., a_k$ are integers such that $0 \leq a_i < n_i$for every i, then there is one and only one integer x, such that $0 \leq x < N$ and the remainder of the Euclidean division of x by $n_i$is a_i for every i.

This may be restated as follows in term of congruences: If the n_i are pairwise coprime, and if $a_1, ..., a_k$ are any integers, then there exists an integer x such that

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned},$$

and any two such x are congruent modulo N.

In abstract algebra, the theorem is often restated as: if the n_i are pairwise coprime, the map

$$x \bmod N \quad \mapsto \quad (x \bmod n_1, \ldots, x \bmod n_k)$$

defines a ring isomorphism[12]

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

between the ring of integers modulo N and the direct product of the rings of integers modulo the n_i. This means that for doing a sequence of arithmetic operations in $\mathbb{Z}/N\mathbb{Z}$ one may do the same computation independently in each $\mathbb{Z}/n_i\mathbb{Z}$ and then get the result by applying the isomorphism (from the right to the left). This may be much faster than the direct computation if *N*and the number of operations are large. This is widely used, under the name *multi-modular computation*, for linear algebraover the integers or the rational numbers.

The theorem can also be restated in the language of combinatorics as the fact that the infinite arithmetic progressions of integers form a Helly family.

10.3. CRT – Problem

An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

This problem can be expressed as a system of congruences

$x\equiv2(\mathrm{mod}3)$

$x\equiv3(\mathrm{mod}5)$

$x\equiv2(\mathrm{mod}7)$

What does (mod n) mean?

$x \equiv a_1 (\mathrm{mod}\ m_1)$

The Chinese remainder theorem states the above equations have a unique solution if the moduli are relatively prime.

Example:

The following is an example of a set of equations with different moduli:

X≡ 2 (mod 3)

X≡ 3 (mod 5)

X≡ 2 (mod 7)

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is x = 23. This value satisfies all equations: 23 ≡ 2 (mod 3), 23 ≡ 3 (mod 5), and 23 ≡ 2 (mod 7).

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.

2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.

3. Find the multiplicative inverse 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

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Note that the set of equations can have a solution even if the moduli are not relatively prime but meet other condition. However , in cryptography only interested in solving equations with coprime moduli.

Example

Find the solution to the simultaneous equations:

solution

We follow the four steps.

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$
3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

Solution for Egg Problem

To solve for x, let $M=3\cdot5\cdot7=105$

M1=35

M2=21

M3=15

Here we see that 2 is an inverse of M1=35 modulo 3 because $35\cdot2\equiv2\cdot2\equiv1(\text{mod}3)$;

1 is an inverse of M2=21 modulo 5, because $21\equiv1(\text{mod}5)$;

and 1 is an inverse of M3=15(mod7), because $15\equiv1(\text{mod}7)$

The solution to this system are those x such that

$x =2\cdot35\cdot2+3\cdot21\cdot1+2\cdot15\cdot1$

$=233 \equiv 23 (\mathrm{mod} 105)$

The answer is 23 eggs.

10.4. The Proof

Let s and t be positive integers with gcd(s, t) = 1 S and t are therefore coprime Prove that there exists an integer w such that sw == 1 (mod t)

For each k, let $M_i = m/m_k$ where $m = m_1 m_2 m_3 \ldots m_k$ (product of mods) Prove that the greatest common denominator of M_i & $m_i = 1$ Or, that M_i and m_i are coprime

Prove that there is an integer x_i such that $m_i x_i == 1 (mod\ m_i)$ and $a_i m_i x_i == a_i$ (mod m_i) Let x == $a_1 m_1 x_1 + a_2 m_2 x_2 + \ldots + a_n m_n x_n$ Prove that $x == a_i (mod\ m_i)$

10.5. Application

In coding theory, detection and correction of errors is done by adding redundancy to data that is sent via a noisy channel or in a computer.

The CRT remainder techniques are useful in developing code that detects errors.

In cryptography, the CRT is used in secret sharing through error-correcting code.

The CRT is itself a secret-sharing scheme without any need for modification

Summary

- Outlined the CRT and their applications in cryptography
- Discussed about the Chinese Remainder Theorem and algorithms
- Worked with various examples related with Chinese Remainder Theorem