IS 5311: Discrete Mathematics

02-Introduction to Number Theory

Lecturer-Ms. M.W.S. Randunu

Department of Interdisiplinary Studies,Faculty of Engineering, University of Ruhuna.

What is a Number theory?

Number theory is a branch of pure mathematics that deals with the properties and relationships of numbers, particularly the integers. It encompasses various topics and subfields, each focusing on different aspects of numbers and their interactions. Here are some key areas within number theory:

1. Prime Numbers
2. Divisibility and Factorization
3. Diophantine Equations
4. Modular Arithmetic

.

Number Sets

- **Natural Numbers** ($\mathbb{N}$): The set of all positive integers.
  Example: $\{1, 2, 3, \ldots\}$
- **Whole Numbers**: The set of natural numbers including zero.
  Example: $\{0, 1, 2, 3, \ldots\}$
- **Integers** ($\mathbb{Z}$): The set of all whole numbers and their negatives.
  Example: $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- **Real Numbers** ($\mathbb{R}$): The set of all rational and irrational numbers.
  Example: $\{\ldots, -1, 0, 1, \sqrt{2}, \pi, \ldots\}$

Well-ordered Property

A set S is said to be **Well-Ordered** if every non-empty subset of S has a least element. This means there is a specific smallest element in each subset when the elements are ordered.

Example: USB drive capacities in GB: $\{16, 32, 64, 128\}$ have least element 16, so the set is well-ordered.

Division

Definition 1:

Let a and b be integers with $a \neq 0$. We say that a divides b, if there is an integer c such that $b = ac$. The integers a and c are called the factors of b. If a divides b, we write $a|b$, and if a does not divide b, we write $a \nmid b$.

Example: Determine whether 5 divides 15 and whether 5 divides 24.

Solution: For $5|15$, we check if there exists an integer c such that $15 = 5c$. Since $c = 3$ satisfies the equation, $5|15$.

Exercise: Check if $8 \mid 64$ bytes (cache block size).
Check if $8 \mid 70$ bytes.

Theorem 1:

Let a, b, and c be integers, where $a \neq 0$. Then

(i) if $a|b$ and $a|c$, then $a|(b+c)$;

(ii) if $a|b$, then $a|bc$ for all integers c;

(iii) if $a|b$ and $b|c$, then $a|c$.

Proof:

Corollary 1:

If a, b, and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|mb + nc$ whenever m and n are integers.

Proof:

Since $a|b$ and $a|c$, we have
$b = am'$ and $c = an'$ for some integers m' and n'. Then
$mb + nc = a(mm' + nn')$, where $mm' + nn'$ is an integer.
Hence, $a|mb + nc$.

The Division Algorithm

Theorem 2:

For any two integers a and b, where $b > 0$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof:

Existence:

Consider the set S of all non-negative integers of the form $a - bk$ where k is an integer:

$$S = \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

S is non-empty because we can choose k sufficiently small such that $a - bk$ is non-negative.

By the well-ordering property of the natural numbers, S has a least element, say r.

By definition of S, there exists an integer q such that

$$r = a - bq$$

and

$$r \geq 0.$$

Therefore,

$$a = bq + r.$$

Proof:

We need to show that $r < b$. Assume for the sake of contradiction that $r \geq b$.
If $r \geq b$, then we can write

$$r = b + r'$$

for some $r' \geq 0$.
Substitute this back into the equation $a = bq + r$:

$$a = bq + b + r'$$

$$a = b(q + 1) + r'.$$

Since $r' = r - b$, we have

$$r' < r.$$

This implies r' is a non-negative integer of the form $a - bk$, contradicting the fact that r is the least element of S.

Therefore, our assumption is false and we must have

$$0 \leq r < b.$$

Uniqueness: Suppose there exist integers q, q' and r, r' such that

$$a = bq + r$$

and

$$a = bq' + r',$$

with

$$0 \leq r < b$$

and

$$0 \leq r' < b.$$

Then,

$$bq + r = bq' + r'.$$

Rearranging gives

$$b(q - q') = r' - r.$$

This implies $b \mid (r' - r)$.
Since $0 \leq r, r' < b$, the only way b can divide $r' - r$ is if $r' - r = 0$, meaning

$$r' = r.$$

Therefore,

$$b(q - q') = 0.$$

Since $b > 0$, we have

$$q = q'.$$

Hence, the integers q and r are unique.

Definition 2:

In the equality given in the division algorithm, b is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } b, \quad r = a \textbf{ mod } b.$$

Remark:

- a **mod** b. is defined to be the remainder when a is divided by b.
- q = a **div** b is defined to be the integer quotient when a is divided by b.

Example: Find the quotient and remainder when 101 is divided by 11.

Solution: Here we can use the division algorithm:

$$\text{dividend} = \text{divisor} \times \text{quotient} + \text{remainder}$$

Given:

- Dividend (a): 101
- Divisor (b): 11

We want to find the quotient (q) and remainder (r).
Using the division algorithm, we have:

$$101 = 11 \times q + r$$

To find q, we calculate $q = \text{dividend} \operatorname{div} \text{divisor}$, and to find r, we calculate $r = \text{dividend} \bmod \text{divisor}$.

$$q = 101 \operatorname{div} 11 = 9 \quad \text{(quotient)}$$

$$r = 101 \bmod 11 = 2 \quad \text{(remainder)}$$

Exercise: Find the quotient and remainder when 123 is divided by 7.

Exercise: -25 is divided by 7, the quotient and remainder are?

Exercise: Find q and r when 512 is divided by 64 (memory blocks).

Exercise: Find q and r when -45 is divided by 12 (signed byte offset).

Primes

Definition 3:

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Remark:

The integer n is composite if and only if there exists an integer a such that a divides n and $1 < a < n$.

The number 13 is prime because its only positive factors are 1 and 13, whereas the number 15 is composite because it is divisible by 3 and 5.

Theorem 3:: The Fundamental Theorem Of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Example: The prime factorizations of 48, 60, 72, and 90 are given by

$$48 = 2^4 \cdot 3$$
$$60 = 2^2 \cdot 3 \cdot 5$$
$$72 = 2^3 \cdot 3^2$$
$$90 = 2 \cdot 3^2 \cdot 5$$

Theorem 4:

There are infinitely many primes.

Proof:

We will prove this theorem using a proof by contradiction.
We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$.
Let

$$Q = p_1 p_2 \ldots p_n + 1.$$

Proof:Ctd...

By the fundamental theorem of arithmetic,
Q is prime or else it can be written as the product of two or more primes.
However, none of the primes p_j divides Q, for if $p_j | Q$, then p_j divides $Q - p_1 p_2 \dots p_n = 1$.
Hence, there is a prime not in the list $p_1, p_2, \dots, p_n$.
This prime is either Q, if it is prime, or a prime factor of Q.
This is a contradiction because we assumed that we have listed all the primes.
Consequently, there are infinitely many primes.

Trial Division

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Example:
Consider the composite number $n = 45$. The square root of 45 is approximately 6.7. The prime numbers less than or equal to 6.7 are 2, 3, and 5.
We check each prime number:

- 45 is not divisible by 2.
- 45 is divisible by 3 (since $45 \div 3 = 15$).

Therefore, 45 has a prime divisor (3) that is less than or equal to $\sqrt{45}$.

Conjectures and Open Problems About Primes

Goldbach's Conjecture

Every even integer greater than 2 is the sum of two primes.

- $6 = 3 + 3$
- $8 = 5 + 3$
- $10 = 7 + 3$
- $12 = 7 + 5$
- $20 = 13 + 7$
- $22 = 19 + 3$

Conjectures and Open Problems About Primes

The Twin Prime Conjecture

There are infinitely many twin primes.

Twin primes are pairs of primes that differ by 2/

Examples: (29, 31), (41, 43), (59, 61)

Greatest Common Divisor

The largest integer that divides both of two integers is called the **greatest common divisor** of these integers.

Definition 4:

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Example: What is the greatest common divisor of 24 and 36?

Solution:

First, we list the divisors of 24 and 36:

$$\text{Divisors of 24: } 1, 2, 3, 4, 6, 8, 12, 24$$

$$\text{Divisors of 36: } 1, 2, 3, 4, 6, 9, 12, 18, 36$$

Next, we identify the common divisors:

$$\text{Common divisors of 24 and 36: } 1, 2, 3, 4, 6, 12$$

Finally, we select the largest common divisor:

The greatest common divisor (gcd) of 24 and 36 is 12.

Therefore, the gcd of 24 and 36 is $\boxed{12}$.

Exercise: What is the greatest common divisor of 17 and 22?

Solution:

Exercise: gcd $(2048, 3072)$

Solution:

Exercise: gcd $(128, 512)$

Solution:

Definition 5:

The integers a and b are relatively prime if their greatest common divisor is 1.

Definition 6:

The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example: 64, 81, 125 have no common factor other than 1.

Example: Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: For the integers 10, 17, and 21:

$$\gcd(10, 17) = 1$$
$$\gcd(10, 21) = 1$$
$$\gcd(17, 21) = 1$$

Since the gcd of each pair is 1, the integers 10, 17, and 21 are pairwise relatively prime.
For the integers 10, 19, and 24:

$$\gcd(10, 19) = 1$$
$$\gcd(10, 24) = 2$$
$$\gcd(19, 24) = 1$$

The integers 10 and 19 are relatively prime, but the gcd of 10 and 24 is 2, not 1. Therefore, the integers 10, 19, and 24 are not pairwise relatively prime.

Another method to determine the greatest common divisor

Let the prime factorizations of the positive integers a and b be:

$$a = p_{a1}^{a_1} \cdot p_{a2}^{a_2} \cdot \ldots \cdot p_{an}^{a_n}, \quad b = p_{b1}^{b_1} \cdot p_{b2}^{b_2} \cdot \ldots \cdot p_{bn}^{b_n},$$

where each exponent is a nonnegative integer. All primes present in either factorization are included in both, with zero exponents if necessary. Then, the gcd of a and b, denoted as $\gcd(a, b)$, is given by:

$$\gcd(a, b) = p_{\min(a1,b1)}^{\min(a1,b1)} \cdot p_{\min(a2,b2)}^{\min(a2,b2)} \cdot \ldots \cdot p_{\min(an,bn)}^{\min(an,bn)},$$

where $\min(x, y)$ represents the minimum of the two numbers x and y. This formula for $\gcd(a, b)$ is valid because the integer on the right-hand side divides both a and b. Additionally, no larger integer can divide both a and b because the exponents of the primes in this factorization cannot be increased, and no other primes can be included.

Example: Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is given by:

$$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20.$$

Least Common Multiple

Definition 7:

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

Suppose the prime factorizations of a and b are as before. Then the least common multiple of a and b is given by:

$$\text{lcm}(a, b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_n^{\max(a_n,b_n)},$$

where $\max(x, y)$ denotes the maximum of the two numbers x and y.
This formula is valid because a common multiple of a and b has at least $\max(a_i, b_i)$ factors of p_i in its prime factorization, and the least common multiple has no other prime factors besides those in a and b.

Theorem 5:

Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

Example: Find the least common multiple (lcm) of 24 and 36 using their prime factorizations.

Solution: Let's find the prime factorization of each number:

$$24 = 2^3 \times 3^1$$
$$36 = 2^2 \times 3^2$$

Now, we construct the lcm by taking the maximum exponent for each prime factor:

$$\text{lcm}(24, 36) = 2^3 \times 3^2 = 72.$$

So, the least common multiple of 24 and 36 is 72.

Example: $\text{lcm}\ (120, 144) = 720$

The Euclidean Algorithm

To compute the greatest common divisor (gcd) of two numbers using the Euclidean algorithm, we can follow these steps:

1. Divide the larger number by the smaller number.
2. Replace the larger number with the smaller number and the smaller number with the remainder of the division.
3. Repeat the process until the remainder is 0.
4. The last non-zero remainder is the gcd.

To find $\gcd(91, 287)$:

- Divide the larger number, 287, by the smaller number, 91:

$$287 = 91 \times 3 + 14$$

- Since any divisor of 91 and 287 must also divide their difference, which is 14, we now focus on finding the gcd of 91 and 14.
- Divide 91 by 14:

$$91 = 14 \times 6 + 7$$

- Now, we focus on finding the gcd of 14 and 7.
- Divide 14 by 7:

$$14 = 7 \times 2$$

- Since 7 divides 14, the gcd of 14 and 7 is 7.
- Therefore, the gcd of 91 and 287 is also 7.

Lemma 1:

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Proof:

Example: Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.
Solution: Successive uses of the division algorithm give:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248, \\ 414 &= 248 \cdot 1 + 166, \\ 248 &= 166 \cdot 1 + 82, \\ 166 &= 82 \cdot 2 + 2, \\ 82 &= 2 \cdot 41 + 0. \end{aligned}$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

Exercise: Find the greatest common divisor of the following pairs using the Euclidean algorithm:

1. 960 and 1440
2. 414 and 662
3. 252 and 198
4. 1500 and 2000
5. 150 and 35
6. 48 and 18

Modular Arithmetic

The notation $a \mod m$ represents the remainder when a is divided by the positive integer m. We now introduce another related notation to indicate that two integers have the same remainder when divided by m.

Definition 8:

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a is congruent to b modulo m.
We say that $a \equiv b \pmod{m}$ is a congruence and that m is its modulus.If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Example: System repeats every 256 ticks. Tick 514 is same as tick 2.

Example:

$$17 \equiv 2 \pmod 5 \quad \text{as} \quad 17 - 2 = 5 \times 3,$$

and

$$-8 \equiv 2 \pmod 5 \quad \text{as} \quad -8 - 2 = 5 \times (-2).$$

Theorem 6:

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

Theorem 7:

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

If $a \equiv b \pmod{m}$, by the definition of congruence, we know that $m \mid (a - b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$.

Conversely, if there is an integer k such that $a = b + km$, then $a - b = km$. Since k is an integer, this implies that $m \mid (a - b)$. Hence, by the definition of congruence, $a \equiv b \pmod{m}$.

Note:

(i) $a \equiv a \pmod{m}$ for any $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

(ii) $a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

For: Let $a = mq_1 + r_1$ and $b = mq_2 + r_2$, where $0 \leq r_1, r_2 < m$ and $q_1, q_2, r_1, r_2 \in \mathbb{Z}$.
Then,

$$a - b = m(q_1 - q_2) + (r_1 - r_2) \quad \cdots \quad (1)$$

"$\Rightarrow$"
If $a \equiv b \pmod{m}$, this implies $m \mid (a - b)$. Therefore, by equation (1), $m \mid (r_1 - r_2)$.
Since $0 \leq |r_1 - r_2| < m$, we must have $r_1 - r_2 = 0$, which means $r_1 = r_2$.
"$\Leftarrow$"
If $r_1 = r_2$, then equation (1) becomes:

$$a - b = m(q_1 - q_2).$$

Thus, $a \equiv b \pmod{m}$.

Theorem 8:

Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

(i) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff -a \equiv -b \pmod{m} \iff a - b \equiv 0 \pmod{m}$.

(ii) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.

(iii) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \implies ax + cy \equiv bx + dy \pmod{m}$ for any $x, y \in \mathbb{Z}$.

(iv) $a \equiv b \pmod{m}$ and $n \mid m$ for $n \in \mathbb{Z}^+ \implies a \equiv b \pmod{n}$.

(v) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$.

Theorem 9:

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

Proof:

Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 7, there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Hence,

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

Example: Because $14 \equiv 4 \pmod 5$ and $9 \equiv 4 \pmod 5$, it follows from Theorem 9 that

$$23 = 14 + 9 \equiv 4 + 4 = 8 = 5 + 3 \equiv 3 \pmod 5$$

and that

$$126 = 14 \cdot 9 \equiv 4 \cdot 4 = 16 = 15 + 1 \equiv 1 \pmod 5.$$

Corollary 2

Let m be a positive integer and let a and b be integers. Then

$$(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

and

$$ab \mod m = ((a \mod m)(b \mod m)) \mod m.$$

Proof:

By the definitions of $\mod m$ and of congruence modulo m, we know that

$$a \equiv (a \mod m) \pmod{m} \quad \text{and} \quad b \equiv (b \mod m) \pmod{m}.$$

Hence, Theorem 9 tells us that

$$a + b \equiv (a \mod m) + (b \mod m) \pmod{m}$$

and

$$ab \equiv (a \mod m)(b \mod m) \pmod{m}.$$

Linear Congruences

A linear congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers.
To solve this linear congruence and find all integers x that satisfy it, one method utilizes an integer $\overline{a}$ such that

$$\overline{a}a \equiv 1 \pmod{m},$$

provided such an integer exists. This $\overline{a}$ is referred to as an **inverse** of a modulo m. The existence of an inverse of a modulo m is guaranteed whenever a and m are relatively prime, as ensured by Theorem 10.
By finding a^{-1}, the solution to the linear congruence $ax \equiv b \pmod{m}$ can be expressed as

$$x \equiv a^{-1}b \pmod{m},$$

Theorem 10:

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Proof:

Since $\gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.$$

This implies that

$$sa + tm \equiv 1 \pmod{m}.$$

Because $tm \equiv 0 \pmod{m}$, it follows that

$$sa \equiv 1 \pmod{m}.$$

Consequently, s is an inverse of a modulo m.

Solving Congruences

Example: Find an inverse of 3 modulo 7.

Solution: we need to find an integer a such that $3a \equiv 1 \pmod 7$.

We can simply try all integers from 0 to 6 until we find one that satisfies the congruence. Let's check:

$$3 \cdot 0 \equiv 0 \not\equiv 1 \pmod 7$$
$$3 \cdot 1 \equiv 3 \not\equiv 1 \pmod 7$$
$$3 \cdot 2 \equiv 6 \not\equiv 1 \pmod 7$$
$$3 \cdot 3 \equiv 9 \equiv 2 \not\equiv 1 \pmod 7$$
$$3 \cdot 4 \equiv 12 \equiv 5 \not\equiv 1 \pmod 7$$
$$3 \cdot 5 \equiv 15 \equiv 1 \pmod 7$$

So, 5 is an inverse of 3 modulo 7.

Exercise: Solve the following linear congruences

1. $3x \equiv 4 \pmod{7}$
2. $5x \equiv 3 \pmod{11}$
3. $9x \equiv 4 \pmod{26}$

Example: Find an inverse of 101 modulo 4620

Solution: we can use the Euclidean algorithm to compute the greatest common divisor of 101 and 4620. If the greatest common divisor is 1, then 101 and 4620 are relatively prime, and 101 has an inverse modulo 4620.
Using the Euclidean algorithm:

$$\begin{aligned} 4620 &= 45 \times 101 + 75 \\ 101 &= 1 \times 75 + 26 \\ 75 &= 2 \times 26 + 23 \\ 26 &= 1 \times 23 + 3 \\ 23 &= 7 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Here 1 is the greatest common divisor of 101 and 4620. Therefore, 101 and 4620 are relatively prime, and 101 has an inverse modulo 4620.

Now, we can use the extended Euclidean algorithm to find the coefficients s and t such that $101s + 4620t = 1$.
The coefficient s will be the inverse of 101 modulo 4620.
Working backward from the equations derived in the Euclidean algorithm:

$$
\begin{aligned}
1 &= 3 - 1 \times 2 \\
&= 3 - 1 \times (23 - 7 \times 3) \\
&= 8 \times 3 - 1 \times 23 \\
&= 8 \times (26 - 1 \times 23) - 1 \times 23 \\
&= 8 \times 26 - 9 \times 23 \\
&= 8 \times 26 - 9 \times (75 - 2 \times 26) \\
&= 26 \times 26 - 9 \times 75 \\
&= 26 \times (101 - 75) - 9 \times 75 \\
&= 26 \times 101 - 35 \times 75 \\
&= 26 \times 101 - 35 \times (4620 - 45 \times 101) \\
&= 1761 \times 101 - 35 \times 4620
\end{aligned}
$$

Thus, we find that the inverse of 101 modulo 4620 is 1626.
Therefore, the inverse of 101 modulo 4620 is 1626.

Exercise: Find an inverse of 17 modulo 1001

Chinese Remainder Theorem (CRT)

The Chinese Remainder Theorem (CRT) is a fundamental result in number theory with origins in ancient Chinese mathematics. It provides a way to solve systems of simultaneous congruences with pairwise coprime moduli. CRT has both theoretical elegance and practical applications in modern computer science and cryptography.

The CRT was first introduced by the Chinese mathematician **Sun Zi** in the 3rd century AD in his work *Sunzi Suanjing*. He posed a problem:

> *"There is a number that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7. What is the number?"*

This is now recognized as an early instance of the CRT. Later, the theorem was formalized by **Aryabhata** in 5th century India and studied by Islamic and European mathematicians. The name "Chinese Remainder Theorem" became standard in the 20th century due to its historical origin.

Theorem Statement

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers (i.e., $\gcd(m_i, m_j) = 1$ for $i \neq j$), and let $a_1, a_2, \ldots, a_k$ be any integers. Then the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

To solve the system of congruences:

$$x \equiv a_i \pmod{m_i}, \quad \text{for } i = 1, 2, \ldots, k,$$

follow these steps:

- Compute the product of all moduli:

$$M = m_1 m_2 \cdots m_k$$

- For each i, compute:

$$M_i = \frac{M}{m_i}$$

- Find the modular inverse y_i of M_i modulo m_i, i.e.:

$$M_i y_i \equiv 1 \pmod{m_i}$$

- Compute the solution using:

$$x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod{M}$$

Solve the system:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 4$$
$$x \equiv 1 \pmod 5$$

Step 1: $M = 3 \cdot 4 \cdot 5 = 60$

Step 2:

$$M_1 = \frac{60}{3} = 20, \quad M_2 = \frac{60}{4} = 15, \quad M_3 = \frac{60}{5} = 12$$

Step 3: Find modular inverses:

- $20y_1 \equiv 1 \pmod 3 \Rightarrow 2y_1 \equiv 1 \Rightarrow y_1 = 2$
- $15y_2 \equiv 1 \pmod 4 \Rightarrow 3y_2 \equiv 1 \Rightarrow y_2 = 3$
- $12y_3 \equiv 1 \pmod 5 \Rightarrow 2y_3 \equiv 1 \Rightarrow y_3 = 3$

Step 4: Compute:

$$x \equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 \pmod{60}$$

$$x \equiv 80 + 135 + 36 = 251 \pmod{60}$$

$$\boxed{x \equiv 11 \pmod{60}}$$

CRT plays an important role in both pure and applied mathematics. Some key applications include:

1. **Cryptography**
2. **Computer Arithmetic**
3. **Modular Equation Solving**
4. **Error Detection and Correction**
5. **Scheduling and Calendars**
6. **Abstract Algebra**

Thank You

Any Questions?