Theorem 3.3.6. **(Fundamental theorem of Arithmetic)**

Any positive integer is either 1, or a prime, or it can be expreesed as a product of primes, the representation being unique except for the order of the prime factors.

Proof. Let n be a positive integer. Either $n = 1$ or $n > 1$. Let $P(n)$ be the statement that $n(> 1)$ is either a prime, or it can be expressed as a product of primes.

$P(2)$ is true, since 2 is a prime.

Let us assume that $P(n)$ is true for all n, where n is a positive integer such that $2 \leq n \leq k$.

If $k + 1$ be itself a prime then $P(k + 1)$ is true and by the second principle of induction, $P(n)$ is true for all positive integers $n > 1$.

If $k+1$ be not a prime then it is a composite number. Let $k+1 = rs$ where r, s are integers with $2 \leq r < k+1, 2 \leq s < k+1$.

By induction hypothesis, $P(r)$ and $P(s)$ are both true. Then

$r = p_1p_2 \ldots p_i$ where $p_1, p_2, \ldots, p_i$ are primes, $i \geq 1$;

$s = q_1q_2 \ldots q_j$ where $q_1, q_2, \ldots, q_j$ are primes, $j \geq 1$.

Thus $k + 1$ is exprdssed as the product of primes and $P(k + 1)$ is proved to be true. By the second principle of induction $p(n)$ is true for all positive integers $n > 1$.

Hence the first part of the theorem is established.

In order to prove uniqueness of the representation, let us assume that $n = p_1p_2 \ldots p_k = q_1q_2 \ldots q_m$, where p_i and q_i are all primes.

Since $p_1 \mid n$, it follows that $p_1 \mid q_1q_2 \ldots q_m$.

Since p_1 is a prime, $p_1 \mid q_r$ for some r where $1 \leq r \leq m$. But since p_1 and q_r are both primes, $p_1 = q_r$.

We obtain $p_2p_3 \ldots p_k = q_1q_2 \ldots q_{r-1}q_{r+1} \ldots q_m$.

We repeat the argument with p_2 and obtain $p_2 = q_s$ for some s where $1 \leq s \leq m, s \neq r$. Then

$$p_3p_4 \ldots p_k = q_1q_2 \ldots q_{r-1}q_{r+1} \ldots q_{s-1}q_{s+1} \ldots q_m.$$

If $k < m$, then after k steps the left hand side reduces to 1 and the right hand side becomes the product of $m - k$ q's, each of which is a prime. This cannot happen. Therefore $k \geq m$.

If $k > m$, then after m steps the right hand side reduces to 1 and the left hand side becomes the product of $k - m$ p's, each of which is a prime. This cannot happen. Therefore $k \leq m$.

Hence $k = m$ and the products $p_1p_2 \ldots p_m, q_1q_2 \ldots q_k$ give the same representation except for the order of the factors.

Thus $n(> 1)$ is expressed as the product of a number of primes, the representation being unique except for the order of the factors. □

Note. In the application of the fundamental theorem we write any integer $n(> 1)$ in the form, called *the canonical form*,

$$n = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r},$$

where the primes p_i are distinct with $p_1 < p_2 < \cdots < p_r$ and the exponents α_i are positive.

An integer is said to be *square-free* if no α_i in the canonical form of n is greater than 1.

To illustrate the representation, let us take $n = 210, 3150$.

$$210 = 2.3.5.7, \quad 3150 = 2.3.3.5.5.7 = 2.3^2.5^2.7.$$

Here 210 is square free.

then the part (i) of the theorem states that $a \circ (b \star c) = (a \circ b) \star (a \circ c)$ for $a, b \in \mathbb{N}$ and the part (ii) of the theorem states that $a \star (b \circ c) = (a \star b) \circ (a \star c)$ for $a, b \in \mathbb{N}$.

These establish that the operation $\circ$ is distributive over the operation $\star$ and the operation $\star$ is distributive over the operation $\circ$.

Worked Example.

1. If p be a prime, show that $\sqrt{p}$ is not a rational number.

Since p is a prime, p is an integer ≥ 2 and therefore $\sqrt{p} > 1$.

Let $\sqrt{p}$ be a rational number. Then $\sqrt{p} = \frac{m}{n}$ for some natural numbers m, n. We assert that $m > 1$ and $n > 1$, because

$m = 1$ and $n = 1 \Rightarrow p = 1^2 = 1$, a contradiction

$m > 1$ and $n = 1 \Rightarrow p = m.m$ and therefore p is not a prime, a contradiction

$m = 1$ and $n > 1 \Rightarrow \sqrt{p} < 1$, a contradiction.

Therefore $m > 1$ and $n > 1$. We also have $pn^2 = m^2$. The number of primes in the factorisation of m being unique by the fundamental theorem of arithmetic, it follows that the number of primes (counting multiplicity) in the factorisation of m^2 is always even.

Similarly, the number of primes in the factorisation of n^2 is also even. Therefore the number of primes in the factorisation of pn^2 is odd (since p is a prime).

Since $pn^2 = m^2$, it appears that the same integer m^2 is expressed as the product of an odd number of primes in one representation and as the product of an even number of primes in another representation.

This contradicts uniqueness of the number of prime factors in the decompostion.

We conclude that $\sqrt{p}$ is not a rational number.

Theorem 3.3.8. **(Euclid).** The number of primes is infinite.

Proof. We prove the theorem by contradiction.

Let us suppose that the number of primes is finite and let p be the greatest prime. We write the primes $2, 3, 5, 7, \ldots$ in succession and p is the last in the enumeration.

The product $2.3.5\ldots p$ in which every prime appears only once is divisible by each prime and therefore the number $(2.3.5\ldots p) + 1$ is not divisible by any of the primes $2, 3, 5, \ldots, p$.

Hence this number is either itself a prime, or being a composite number, is divisible by a prime number greater than p. In both the cases

p fails to be the greatest prime and therefore the number of primes is infinite. □

Note. Although the number of primes is infinite, there are arbitrarily large gaps in the sequence of primes. For every positive integer k, there exist k consecutive composite numbers. To be explicit, each of the k consecutive integers

$$(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+(k+1)$$

is composite, because $(k+1)!+r$ is divisible by r if $2 \leq r \leq k+1$.

This indicates that the primes are irregularly spaced in the sequence of positive integers. The number of primes less than a positive integer x is denoted by $\pi(x)$. No simple formula for determining $\pi(x)$ has yet been found.

Test for primality.

If a positive integer a be composite, then $a = bc$ for integers b, c satisfying $1 < b < a$, $1 < c < a$. Let $b \leq c$. Then $b^2 \leq bc = a$ and this implies $b \leq \sqrt{a}$.

Since $b > 1$, b has at least one prime divisor p and $p \leq b \leq \sqrt{a}$.

In testing primality of a positive integer n, it is sufficient to divide n by primes not exceeding $\sqrt{n}$.

Greek mathematician, Eratosthenes (276- 494 B.C.) utilised this concept to find all primes less than a given positive integer n. His device is called the " seive of Eratosthenes " which consists in writing all integers from 2 to n in natural order and then striking out all multiples $2p, 3p, 4p, 5p, \ldots$ of all primes $p \leq \sqrt{n}$. The integers that are left in the list (survived the seive) are primes.

For example, in order to determine all primes ≤ 30, the "sieve" method is applied by striking all multiples of $2, 3, 5$ from the table of integers from 2 to 30, since 5 is the largest prime $\leq \sqrt{30}$.

The table is shown below.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~
~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

This method has limitations. If the positive integer n be sufficiently large, the method becomes impracticable.

With the aid of other theorems and with the aid of computers, many mathematicians in recent years have prepared extensive tables of primes. But still the problem of determining all primes by some formula remains open.

3.3.9. The number of positive divisors of a positive integer.

Let n be a positive integer greater than 1. Then n can be expressed as $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, where the primes p_i are distinct with $p_1 < p_2 < \cdots < p_r$ and the exponents α_i are all positive.

If m be a positive divisor of n then m is of the form $p_1^{u_1}p_2^{u_2}\cdots p_r^{u_r}$, where $0 \leq u_1 \leq \alpha_1, 0 \leq u_2 \leq \alpha_2, \ldots, 0 \leq u_r \leq \alpha_r$.

Thus the positive divisors of n are in one-to-one correspondence with the totality of r-tuples $(u_1, u_2, \ldots, u_r)$, where $0 \leq u_1 \leq \alpha_1, 0 \leq u_2 \leq \alpha_2, \ldots, 0 \leq u_r \leq \alpha_r$.

The number of such r-tuples is $(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)$.

Hence the total number of positive divisors of n is $(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)$.

If $n = 1$, then there is only one positive divisor.

Note. The total number of positive divisors $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$ include both the divisors 1 and n.

Definition. The number of positive divisors of a positive integer n is denoted by $\tau(n)$. (*tau n*)

If the canonical form of a positive integer $n(> 1)$ be

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r},$$

then $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)$; and $\tau(1) = 1$.

For example, $\tau(48) = \tau(2^4\,3) = (4 + 1)(1 + 1) = 10$.

Theorem 3.3.10. The total number of positive divisors of a positive integer n is odd if and only if n is a perfect square.

Proof. Let $n(> 1)$ be a perfect square and let the canonical form of n be $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ and α_i are all positive.

Then each of $\alpha_1, \alpha_2, \ldots, \alpha_r$ is an even integer and $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)$ is odd.

If however, $n = 1$, a perfect square, then $\tau(n) = 1$ and it is odd.

Conversely, let $(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_r + 1)$ be odd. Then each of the factors $\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_r + 1$ must be odd. Consequently, each of $\alpha_1, \alpha_2, \ldots, \alpha_r$ must be even and n is therefore a perfect square.

This completes the proof.

3.3.11. The sum of all positive divisors of a positive integer.

Let n be a positive integer greater than 1. Then n can be expressed as $n = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r}$, where the primes p_i are distinct with $p_1 < p_2 < \cdots < p_r$ and $\alpha_i > 0$.

Every positive divisor of n is a term in the product

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_r + \cdots + p_r^{\alpha_r})$$

and conversely, each term in the product is a divisor of n.

Hence the sum of all positive divisors of n

$$= (1+p_1+p_1^2+\cdots+p_1^{\alpha_1})(1+p_2+p_2^2+\cdots+p_2^{\alpha_2})\ldots(1+p_r+p_r^2+\cdots+p_r^{\alpha_r})$$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}.$$

If $n = 1$, the sum $=1$.

Definition. The sum of all positive divisors of a positive integer n is denoted by $\sigma(n)$. (*sigma n*).

If the canonical form of a positive integer $n(> 1)$ be

$$n = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r},$$

then $\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1}$; and $\sigma(1) = 1$.

Definition. A function whose domain is the set of all positive integers is said to be a *number-theoretic function* (or an *arithmetic function*). The range of a number-theoretic function need not be the set of all positive integers. We shall encounter some simple number-theoretic functions which assume positive integral values.

The functions τ and σ are examples of number-theoretic functions.

A number-theoretic function f is said to be *multiplicative* if $f(mn) = f(m)f(n)$ for all integers m, n such that m, n are prime to each other.

Theorem 3.3.12. The functions τ and σ are both multiplicative functions.

Proof. Let m, n be relatively prime integers.

$\tau(mn) = \tau(m)\tau(n)$ holds trivially if either m or n is 1.

We assume $m > 1$ and $n > 1$.

Let $m = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r}$ and $n = q_1{}^{\beta_1} q_2{}^{\beta_2} \ldots q_s{}^{\beta_s}$, where p_i, q_j are primes and $\alpha_i \geq 1$, $\beta_j \geq 1$.

Since m, n are relativey prime, each p_i is different from each q_j.

Therefore the prime factorisation of mn is

$mn = p_1{}^{\alpha_1} p_2{}^{\alpha_2} \ldots p_r{}^{\alpha_r} q_1{}^{\beta_1} q_2{}^{\beta_2} \ldots q_s{}^{\beta_s}$.

$$\tau(mn) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)(\beta_1+1)(\beta_2+1)\ldots(\beta_s+1)$$
$$= \tau(m)\tau(n).$$

$$\sigma(mn) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}.\frac{p_2^{\alpha_2+1}-1}{p_2-1}\ldots\frac{p_r^{\alpha_r+1}-1}{p_r-1}.\frac{q_1^{\beta_1+1}-1}{q_1-1}.\frac{q_2^{\beta_2+1}-1}{q_2-1}\ldots\frac{q_s^{\beta_s+1}-1}{q_s-1}$$
$$= \sigma(m)\sigma(n).$$

Hence τ and σ are multiplicative functions.

Definition. Perfect number. A positive integer n is said to be a *perfect number* if $\sigma(n) = 2n$, i.e., if n be the sum of all its positive divisors excluding itself.

For example, 6 is a perfect number. 28 is another.

Worked Examples.

1. Find $\tau(360)$ and $\sigma(360)$.

$360 = 2^3.3^2.5$. Therefore $\tau(360) = (1+3).(1+2).(1+1) = 24$.

$\sigma(360) = \frac{2^4-1}{2-1}.\frac{3^3-1}{3-1}.\frac{5^2-1}{5-1} = 15.13.6 = 1170.$

2. Find the number of odd positive divisors of 2700.

$2700 = 2^2.3^3.5^2$. Every positive divisor of 2700 is of the form $2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}$, where $0 \le \alpha_1 \le 2, 0 \le \alpha_2 \le 3, 0 \le \alpha_3 \le 2$.

Therefore each term in the product $(1+2+2^2)(1+3+3^2+3^3)(1+5+5^2)$ is a positive divisor of 2700 and conversely.

The odd positive divisors of 2700 are given by the terms of the product $1.(1+3+3^2+3^3)(1+5+5^2)$.

The number of odd positive divisors are $(3+1)(2+1)$, i.e.,12.

3. Find the sum of all even positive divisors of 2700.

From the previous example it follows that the even positive divisors of 2700 are given by the different terms of the product

$$(2+2^2)(1+3+3^2+3^3)(1+5+5^2).$$

The sum of the even positive divisors

$$= (2+2^2)(1+3+3^2+3^3)(1+5+5^2) = 6.40.31 = 7440.$$

4. Let $k > 1$ and $2^k - 1$ is a prime. If $n = 2^{k-1}(2^k-1)$ then show that n is a perfect number.

$2^k - 1$ is an odd prime, say p.

$\sigma(n) = \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p)$, since 2^{k-1} and p are prime to each other.

$\sigma(2^{k-1}) = 1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$ and $\sigma(p) = 1 + p$.

Therefore $\sigma(n) = (2^k-1)(1+p) = (2^k-1)2^k = 2n$.

This proves that n is a perfect number.

Note. This example shows that if $2^n - 1$ $(n > 1)$ is a prime, then the number $2^{n-1}(2^n - 1)$ is a perfect number.

The numbers of the form $M_n = 2^n - 1$ $(n > 1)$ are called Mersenne numbers, named after Mersenne (1588-1648), a French monk and an amateur of mathematics.

The primality of M_n requires n must be a prime.

If M_n be a prime then M_n is called a Mersenne prime and in that case a perfect number $2^{n-1}(2^n - 1)$ is obtained.

5. If $d_1, d_2, \ldots, d_k$ be the list of all positive divisors of a positive integer n, prove that $\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = \frac{\sigma(n)}{n}$.

d_i is a positive divisor $\Rightarrow \frac{n}{d_i}$ is also a positive divisor. As d runs through the set of all positive divisors of n, $\frac{n}{d}$ also does so.

Therefore $\frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_k} = d_1 + d_2 + \cdots + d_k = \sigma(n)$

or, $\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = \frac{\sigma(n)}{n}$.

1. Use the principle of induction to prove that

(i) $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all $n \in \mathbb{N}$,

(ii) $1.1! + 2.2! + \cdots + n.n! = (n + 1)! - 1$ for all $n \in \mathbb{N}$,

(iii) $3^{2n-1} + 2^{n+1}$ is divisible by 7 for all $n \in \mathbb{N}$,

(iv) $3^{4n+2} + 5^{2n+1}$ is divisible by 14 for all $n \in \mathbb{N}$,

(v) $10^{n+1} + 10^n + 1$ is divisible by 3 for all $n \in \mathbb{N}$,

(vi) $2.7^n + 3.5^n - 5$ is divisible by 24 for all $n \in \mathbb{N}$.

3.4. Congruence.

Karl Friedrich Gauss (1777-1855), a celebrated German mathematician, introduced the concept of congruence which laid the foundation of modern theory of numbers.

Definition. Let m be a fixed positive integer. Two integers a and b are said to be *congruent modulo* m if $a-b$ is divisible by m. symbolically this is expressed as $a \equiv b(\text{mod } m)$.

To illustrate, let $m=3$. It is easy to verify that $1 \equiv 4(\text{mod } 3), -2 \equiv 1(\text{mod } 3), 6 \equiv 0(\text{mod } 3), 35 \equiv 2\ (\text{mod } 3)$.

When $a-b$ is not divisible by m, a is said to be *incongruent* to b modulo m. It is expressed as $a \not\equiv b(\text{mod } m)$.

For example, $1 \not\equiv 5(\text{mod } 3), -2 \not\equiv 2(\text{mod } 3)$.

Note. When $m=1$, every two integers are congruent modulo m and this case is not so useful and interesting. Therefore m is usually taken to be a positive integer greater than 1.

Theorem 3.4.1. For any two integers a and b, $a \equiv b(\text{mod } m)$ if and only if a and b leave the same remainder when divided by m.

Proof. Let r be the remainder when a is divided by m. Then there exists some integer q such that $a = qm + r, 0 \leq r < m$.

Since $a \equiv b(\text{mod } m), a-b = km$ where k is an integer.

$$\begin{aligned} \text{Therefore } b = a - km &= (qm+r) - km \\ &= (q-k)m + r \end{aligned}$$

and this shows that b leaves the same remainder r.

Conversely, let r be the same remainder when a and b are divided by m. Then $a = q_1m + r, b = q_2m + r$, where q_1, q_2 are integers and $0 \leq r < m$.

Therefore $(a-b) = (q_1 - q_2)m$, i.e., $m \mid a-b$ and this proves that $a \equiv b(\text{mod } m)$. □

To illustrate, let $m=5$. Since $21 \equiv 4.5 + 1$ and $-14 = -3.5 + 1$, 21 and -14 leave the same remainder upon division by 5. Therefore $21 \equiv -14(\text{mod } 5)$.

Properties.

1. $a \equiv a(\text{mod } m)$.
2. If $a \equiv b(\text{mod } m)$ then $b \equiv a(\text{mod } m)$.
3. If $a \equiv b(\text{mod } m), b \equiv c(\text{mod } m)$ then $a \equiv c\ (\text{mod } m)$.

4. If $a \equiv b \pmod{m}$ then for any integer c

$$\begin{aligned} a+c &\equiv b+c \pmod{m} \\ ac &\equiv bc \pmod{m}. \end{aligned}$$

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$$\begin{aligned} a+c &\equiv b+d \pmod{m} \\ ac &\equiv bd \pmod{m}. \end{aligned}$$

6. If $a \equiv b \pmod{m}$ and $d|m, d > 0$, then $a \equiv b (\text{mod } d)$.

Proofs of properties $1-4$ and 6 are immediate.

Proof. 5. $a \equiv b \pmod{m} \Rightarrow a-b = km$ and
$c \equiv d \pmod{m} \Rightarrow c-d = lm$, where k, l are integers.
$(a+c)-(b+d) = (k+l)m$.

Therefore $a+c \equiv b+d \pmod{m}$ since $k+l$ is an integer.

By property 4,
$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$ and
$c \equiv d \pmod{m} \Rightarrow bc \equiv bd \pmod{m}$.

Therefore $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

Definition. If $a \equiv b \pmod{m}$ then b is said to be a *residue* of a modulo m.

By division algorithm there exist integers q and r satisfying $a = qm+r$ with $0 \leq r \leq m-1$.

Since $a-r = qm$, $a \equiv r \pmod{m}$ and this shows that r is a residue of a modulo m. r is said to be the *least non-negative residue* of a modulo m.

Let a be an arbitrary integer. Upon division by m, a leaves one and only one of the integers $0, 1, 2, \ldots, m-1$ as the remainder.

Therefore whatever the integer a may be, the least non-negative residue of a is one and only one of $0, 1, 2, \ldots, m-1$.

The whole set of integers is divided into m distinct and disjoint subsets, called the *residue classes modulo m*, denoted by $\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{m-1}$ and defined by

$$\begin{aligned} \bar{0} &= \{0, \pm m, \pm 2m, \ldots\} \\ \bar{1} &= \{1, 1 \pm m, 1 \pm 2m, \ldots\} \\ \bar{2} &= \{2, 2 \pm m, 2 \pm 2m, \ldots\} \\ &\cdots \quad \cdots \quad \cdots \\ \overline{m-1} &= \{m-1, (m-1) \pm m, (m-1) \pm 2m, \ldots\}. \end{aligned}$$

Any two integers in a residue class are congruent modulo m and any two integers belonging to two different residue classes are incongruent modulo m.

Theorem 3.4.2. If $a \equiv b(\text{mod } m)$ then $a^n \equiv b^n$ (mod m) for all positive integers n.

Proof. We use the principle of induction to prove the theorem.

The theorem is true for $n = 1$.

Let us assume that the theorem is true for some positive integer k. Then $a^k \equiv b^k(\text{mod } m)$.

Now $a^k \equiv b^k(\text{mod } m)$ and $a \equiv b(\text{mod } m)$ together imply that $a^k.a \equiv b^k.b(\text{mod } m)$, i.e., $a^{k+1} \equiv b^{k+1}(\text{mod } m)$.

This shows that the thoerem is true for the positive integer $k+1$ if we assume it to be true for k.

By the principle of induction, the theorem is true for all positive integers n. □

Note. The converse of the theorem fails to hold.

$a^k \equiv b^k(\text{mod } m)$ does not necessarily imply $a \equiv b(\text{mod } m)$.

$$\begin{aligned} \text{For example, } 9^2 &\equiv 7^2(\text{ mod } 8) \text{ but } 9 \not\equiv 7(\text{ mod } 8) \\ 4^3 &\equiv 7^3(\text{ mod } 9) \text{ but } 4 \not\equiv 7(\text{ mod } 9). \end{aligned}$$

Theorem 3.4.3. If $ax \equiv ay(\text{ mod } m)$ and a is prime to m then $x \equiv y(\text{mod } m)$.

Proof. $ax - ay = km$, where k is an integer

or, $x - y = \frac{km}{a}$.

Since $x - y$ is an integer, $a \mid km$. Since a is prime to m and $a \mid km$, it follows that $a \mid k$. Therefore $k = aq$ where q is an integer.

Hence $x - y = qm$ and this proves the theorem.

Note. $ax \equiv ay(\text{mod } m)$ does not necessarily imply $x \equiv y(\text{mod } m)$.

For example, $3.2 \equiv 3.4(\text{mod } 6)$ does not imply $2 \equiv 4(\text{mod } 6)$.

We can cancel the common factor a freely from both sides of the congruence (mod m) provided a is prime to m.

$3.-2 \equiv 2(\text{mod } 8)$, $3.14 \equiv 2(\text{mod } 8)$.

Cancelling the factor 3 which is prime to 8 we get the correct congruence $-2 \equiv 14(\text{mod } 8)$.

Cancellation is allowed however, in some restricted sense which is provided in the following theorem.

Theorem 3.4.4. If $d = gcd(a, m)$ then $ax \equiv ay (\text{mod } m) \Leftrightarrow x \equiv y$ $(\text{mod } \frac{m}{d})$.

Proof. We have $ax - ay = qm$ where q is an integer.

Since $gcd(a, m) = d$, $a = dr$ and $m = ds$ where r and s are integers prime to each other.

Therefore $drx - dry = qds$ or, $x - y = \frac{qs}{r}$.

Since $x - y$ is an integer, $r \mid qs$. r is prime to s and $r \mid qs$ implies $r \mid q$, i.e., $\frac{q}{r}$ is an integer k.

Therefore $x - y = ks$ and this says $x \equiv y$ $(\text{mod } \frac{m}{d})$.

Conversely, $x \equiv y$ $(\text{mod } \frac{m}{d}) \Rightarrow \frac{m}{d} \mid (x - y) \Rightarrow m \mid d(x - y) \Rightarrow$ $m \mid a(x - y) \Rightarrow ax \equiv ay$ $(\text{mod } m)$.

Corollary. If $ax \equiv ay (\text{mod } m)$ and $a \mid m$ then $x \equiv y$ $(\text{mod } \frac{m}{a})$.

For example, $4.7 \equiv 4.10$ (mod 6). Cancellation of 4 from both sides does not give a correct congruence because 4 is not prime to 6. Since $gcd(4, 6) = 2$, we get the correct congruence $7 \equiv 10$ $(\text{mod } \frac{6}{2})$.

Again, $4.7 \equiv 4.10$ (mod 12). Since $4 \mid 12$, we get the correct congruence $7 \equiv 10$ (mod 3) from the corollary.

Theorem 3.4.5. $x \equiv y$ $(\text{mod } m_i)$, for $i = 1, 2, \ldots, r \Leftrightarrow x \equiv y$ $(\text{mod } m)$, where $m = [m_1, m_2, \ldots, m_r]$, the l.c.m. of $m_1, m_2, \ldots, m_r$.

Proof. $x \equiv y$ $(\text{mod } m_i) \Rightarrow m_i \mid (x - y)$, for $i = 1, 2, \ldots, r$

$\Rightarrow x - y$ is a common multiple of $m_1, m_2, \ldots, m_r$

$\Rightarrow [m_1, m_2, \ldots, m_r] \mid (x - y)$

$\Rightarrow x \equiv y$ $(\text{mod } m)$.

Conversely, $x \equiv y$ $(\text{mod } m) \Rightarrow m \mid (x - y)$

$\Rightarrow m_1 m_2 \ldots m_r \mid (x - y)$

$\Rightarrow m_i \mid (x - y)$, for $i = 1, 2, \ldots, r$

$\Rightarrow x \equiv y$ $(\text{mod } m_i)$, for $i = 1, 2, \ldots, r$.

Corollary. If $x \equiv y$ $(\text{mod } m_1)$, $x \equiv y$ $(\text{mod } m_2)$ and m_1, m_2 are relatively prime then $x \equiv y$ $(\text{mod } m_1 m_2)$.

Theorem 3.4.6. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integral coefficients a_i.

If $a \equiv b$ $(\text{mod } m)$ then $f(a) \equiv f(b)$ $(\text{mod } m)$.

Proof. Since $a \equiv b$ $(\text{mod } m)$, $a^k \equiv b^k$ $(\text{mod } m)$ where k is a positive integer. Therefore $a_i a^k \equiv a_i b^k$ $(\text{mod } m)$, where a_i is an integer.

Adding these congruences for $i = 0, 1, 2, \ldots, n$, we have

$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \equiv a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n (\text{mod } m)$

or, $f(a) \equiv f(b)$ $(\text{mod } m)$. □

3.4.7. Divisibility tests.

1. Let $n = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ where a_k are integers and $0 \leq a_k \leq 9, k = 0, 1, \ldots, m$ be the decimal representation of a positive integer n.

Let $S = a_0 + a_1 + \cdots + a_m, T = a_0 - a_1 + \cdots + (-1)^m a_m$. Then

(i) n is divisible by 2 if and only if a_0 is divisible by 2;

(ii) n is divisible by 9 if and only if S is divisible by 9;

(iii) n is divisible by 11 if and only if T is divisible by 11.

Proof. Let us consider the polynomial

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

(i) We have $10 \equiv 0 (\text{mod } 2)$.

Therefore $f(10) \equiv f(0) (\text{mod } 2)$.

But $f(10) = n$ and $f(0) = a_0$.

Therefore $n - a_0$ is divisible by 2.

Hence n is divisible by 2 if and only if a_0 is divisible by 2.

(ii) We have $10 \equiv 1 (\text{mod } 9)$.

Therefore $f(10) \equiv f(1) (\text{mod } 9)$.

But $f(10) = n$ and $f(1) = S$.

Therefore $n \equiv S (\text{mod } 9)$.

This proves that $N - S$ is divisible by 9.

Hence n is divisible by 9 if and only if S is divisible by 9.

(iii) We have $10 \equiv -1 (\text{mod } 11)$.

Therefore $f(10) \equiv f(-1) (\text{mod } 11)$.

But $f(10) = n$ and $f(-1) = T$.

Therefore $n \equiv T (\text{mod } 11)$.

This proves that $n - T$ is divisible by 11.

Hence n is divisible by 11 if and only if T is divisible by 11.

For example, 35078571 is divisible by 9 since the sum of the digits $3 + 5 + 0 + 7 + 8 + 5 + 7 + 1 (= 36)$ is divisible by 9.

It is also divisible by 11 because the sum $1 - 7 + 5 - 8 + 7 - 0 + 5 - 3 (= 0)$ is divisible by 11.

The number 23572 is divisible by 2, since the integer a_0 in the units place is 2 which is divisible by 2. It is not divisible by 9, since the sum $2 + 3 + 5 + 7 + 2 (= 19)$ is not divisible by 9. It is not divisible by 11, since the sum $2 - 7 + 5 - 3 + 2 (= -1)$ is not divisible by 11.

2. Let $n = a_m(1000)^m + a_{m-1}(1000)^{m-1} + \cdots + a_1(1000) + a_0$ where a_k are integers and $0 \leq a_k \leq 999, k = 0, 1, \ldots, m$ be the representation of a positive integer n.

Let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then

(i) n is divisible by 7 if and only if T is divisible by 7,

(ii) n is divisible by 13 if and only if T is divisible by 13,

(iii) n is divisible by 11 if and only if T is divisible by 11.

Proof. Let us consider the polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0.$$

(i) We have $1000 \equiv -1 (\text{mod } 7)$ since $1001 \equiv 7.11.13$.

Therefore $f(1000) \equiv f(-1) (\text{mod } 7)$.

But $f(1000) = n$ and $f(-1) = T$.

Therefore $n \equiv T (\text{mod } 7)$.

This implies $n - T$ is divisible by 7.

Hence n is divisible by 7 if and only if T is divisible by 7.

(ii) and (iii) Similar proofs.

To illustrate, let us consider the number $n = 23146123$. n can be expressed as $23(1000)^2 + 146(1000) + 123$.

n is divisible by 7 because the sum $123 - 146 + 23 = 0$ is divisible by 7.

The same argument proves that n is also divisible by 13 and 11.

Worked Examples.

1. Find the least positive residues in $3^{36} (\text{mod } 77)$.

$3^4 \equiv 4(\text{ mod } 77)$

Therefore $3^{12} \equiv 4^3(\text{ mod } 77) = -13(\text{ mod } 77)$.

This gives $3^{24} \equiv 169(\text{ mod } 77) = 15(\text{ mod } 77)$

Therefore $3^{36} \equiv 15. - 13(\text{ mod } 77) = 36(\text{ mod } 77)$.

Hence the least positive residue is 36.

2. Use the theory of congruences to prove that $7 \mid 2^{5n+3} + 5^{2n+3}$ for all $n \geq 1$.

$2^{5n+3} + 5^{2n+3} = 8.32^n + 125.25^n$.

$32^n - 25^n \equiv 0 (\text{mod } 7)$ for all $n \geq 1$.

Therefore $8.32^n - 8.25^n \equiv 0 \ (\text{mod } 7)$ for all $n \geq 1$.

Also we have $133(25)^n \equiv 0 \ (\text{mod } 7)$ for all $n \geq 1$.

Therefore $8.32^n + 125.25^n \equiv 0 \ (\text{mod } 7)$ for all $n \geq 1$.

This implies $7 \mid 2^{5n+3} + 5^{2n+3}$ for all $n \geq 1$.

3. Prove that $19^{20} \equiv 1(\bmod 181)$.

We have
$$\begin{aligned} 19^2 &\equiv -1(\bmod 181), \text{ whence} \\ 19^{20} &\equiv (-1)^{10}(\bmod 181), \text{ by theorem 3.4.2} \\ \text{or, }\ 19^{20} &\equiv 1(\bmod 181). \end{aligned}$$

4. Prove that $3.4^{n+1} \equiv 3(\bmod 9)$ for all positive integers n.

$$\begin{aligned} 3.4^{n+1} &= 12.4^n = 9.4^n + 3.4^n \\ 3.4^n &= 12.4^{n-1} = 9.4^{n-1} + 3.4^{n-1} \\ \ldots &\ \ldots\ \ldots \\ 3.4^2 &= 12.4 = 9.4 + 3.4 \\ 3.4 &= 12 = 9 + 3. \end{aligned}$$

Therefore $3.4^{n+1} = 9(1 + 4 + 4^2 + \cdots + 4^n) + 3$.

Hence $3.4^{n+1} \equiv 3(\bmod 9)$.

5. Find the remainder when $1! + 2! + 3! + \cdots + 50!$ is divided by 15.

$5! \equiv 0(\bmod 15)$ and for any positive integer n, $(5+n)! \equiv 0(\bmod 15)$. Therefore $1! + 2! + 3! + \cdots + 50! \equiv (1! + 2! + 3! + 4!)\ (\bmod 15)$.
Now $1! + 2! + 3! + 4! = 33 = 15.2 + 3$.
This shows that $33 \equiv 3(\bmod 15)$ and therefore
$1! + 2! + 3! + \cdots + 50! = 3(\bmod 15)$.

3.4.8. Linear congruence.

Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n (n \geq 1)$ be a polynomial with integer coefficients $a_0, a_1, \ldots, a_n$ with $a_0 \not\equiv 0(\bmod m)$. Then $f(x) \equiv 0(\bmod m)$ is said to be a *polynomial congruence* (mod m) of *degree n*.

If there exists an integer x_0 such that $f(x_0) \equiv 0(\bmod m)$, then x_0 is said to be *a solution* of the congruence.

By earlier theorems, if x_1 be any integer satisfying $x_1 \equiv x_0\ (\bmod m)$, then we also have $f(x_1) \equiv 0(\bmod m)$, showing that x_1 is another solution of the congruence.

Thus if one solution be found then infinitely many solutions can be obtained, but all these solutions belong to the same x_0-residue class modulo m and they are not counted as different solutions.

Two solutions x_1, x_2 of $f(x) \equiv 0(\bmod m)$ are said to be *distinct* solutions if $x_1 \not\equiv x_2(\bmod m)$.

Therefore, by the number of solutions of a congruence (mod m) we mean the number of solutions *incongruent in pairs*.

For example, let us consider the congruence $x^2 \equiv 1(\bmod 8)$. $x = 1$ is a solution of the congruence and all solutions congruent to 1(mod

8), i.e., $x = 1 + 8k$, k being an integer are solutions of the congruence.

$x = 3$ is a solution of the congruence and all solutions congruent to 3(mod 8), i.e., $x = 3 + 8k$, k being an integer are solutions of the congruence.

Similarly, $x = 5$, $x = 7$ are solutions of the congruence.

These four solutions of the congruence are distinct, because no two of the solutions are congruent modulo 8.

There cannot be more than m distinct solutions of the congruence, since there are only m different residue classes. If m is small it is an easy job to find all the distinct solutions by direct substitution $x = 1$, $x = 2, \dots, x = m - 1$.

There are many points of difference between a polynomial congruence modulo a positive integer $m > 1$ and the polynomial equation over the field of complex numbers.

A congruence may have no solution. For example, the congruence $x^2 \equiv 3(\bmod 5)$ has no solution which can be established by directly verifying that none of $x = 0$, $x = 1$, $x = 2$, $x = 3$, $x = 4$ satisfies the congruence. In contrast, a polynomial equation has always a solution.

A congruence may have more distinct solutions than its degree. For example, the congruence $x^2 \equiv 1(\bmod 8)$ has four distinct solutions $x = 1, x = 3$, $x = 5$, $x = 7$. In contrast, a polynomial equation of degree m over the complex field has exactly m solutions.

There is an explicit method of solving a congruence of any degree modulo a positive integer $m > 1$. [just by substitution of each of the integers $1, 2, \dots, m - 1$, in turn.] But there is no such explicit method for solving a polynomial equation of degree greater than 4.

Definition.

A polynomial congruence of degree 1 is said to be a *linear congruence*. The general form of a linear congruence modulo a positive integer $m > 1$ is $ax \equiv b(\bmod m)$, where $a \not\equiv 0(\bmod m)$.

An integer c is said to be a *solution* of the linear congruence $ax \equiv b($ mod $m)$ if $ac \equiv b(\bmod m)$.

Theorem 3.4.9. If x_1 be a solution of the linear congruence $ax \equiv b$ (mod m) and if $x_2 \equiv x_1(\bmod m)$, then x_2 is also a solution of the congruence.

Proof. x_1 is a solution $\Rightarrow ax_1 \equiv b(\bmod m)$.

$x_2 \equiv x_1 \pmod{m} \Rightarrow ax_2 \equiv ax_1 \pmod{m}$
$\Rightarrow ax_2 \equiv b \pmod{m}$
$\Rightarrow x_2$ is a solution of the congruence $ax \equiv b \pmod{m}$.

Note. If x_1 be a solution of the congruence $ax \equiv b(\bmod m)$ then $x_1 + \lambda m$ is also a solution for $\lambda = 0, \pm 1, \pm 2, \ldots$. All these solutions belong to one residue class modulo m and these are not counted as different solutions.

Theorem 3.4.10. If $gcd(a, m) = 1$, then the linear congruence $ax \equiv b(\bmod m)$ has a *unique* solution.

Proof. Since $gcd(a, m) = 1$, there exist integers u, v such that $au + mv = 1$. Therefore $a(bu) + m(bv) = b$. This gives $a(bu) \equiv b(\bmod m)$.

This shows that $x = bu$ is a solution of the congruence $ax \equiv b(\bmod m)$.

Let x_1, x_2 be solutions of the congruence $ax \equiv b \pmod{m}$.

Then $ax_1 \equiv b \pmod{m}$ and $ax_2 \equiv b \pmod{m}$.

This implies $ax_1 \equiv ax_2 \pmod{m} \Rightarrow x_1 \equiv x_2 \pmod{m}$, since $gcd(a, m) = 1$.

This proves that the congruence has a unique solution.

Note. The solutions are $x = bu + \lambda m$, where $\lambda = 0, \pm 1, \pm 2, \ldots$ and they all belong to *one and only one* residue class modulo m.

Theorem 3.4.11. If $gcd(a, m) = d$, then the linear congruence $ax \equiv b(\bmod m)$ has no solution if d is not a divisor of b.

If d be divisor of b, then the linear congruence $ax \equiv b \pmod{m}$ has d incongruent solutions $\pmod{m}$.

Proof. Let $ax \equiv b \pmod{m}$ has a solution $x = u$. Then $au \equiv b \pmod{m}$ and this implies $m \mid (b - au)$.

$d \mid m \Rightarrow d \mid (b - au)$. $d \mid a$ and $d \mid (b - au) \Rightarrow d$ is a divisor of b. Contrapositively, d is not a divisor of b implies $ax \equiv b(\bmod m)$ has no solution.

Second part. $d \mid b$. For an integer u, $au \equiv b \pmod{m}$ holds if and only if $\frac{a}{d}u \equiv \frac{b}{d}(\bmod \frac{m}{d})$, by Theorem 3.4.4.

$gcd(\frac{a}{d}, \frac{m}{d}) = 1$ and therefore the congruence $\frac{a}{d}u \equiv \frac{b}{d}(\bmod \frac{m}{d})$ has just one solution $u = x_1(\bmod \frac{m}{d})$.

In other words, the solution of the congruence $\frac{a}{d}u \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ are the integers $u \equiv x_1 \pmod{\frac{m}{d}}$, i.e., $u = x_1 + \frac{m}{d}t, \quad t = 0, \pm 1, \pm 2, \cdots$

If t assumes the values $0, 1, 2, \ldots, d - 1$, then u assumes d values

$x_1, x_1 + \frac{m}{d}, x_1 + \frac{2m}{d}, \ldots, x_1 + \frac{(d-1)m}{d}$ ... (i)

We now show that the integers in the list (i) are incongruent modulo m, while each of all other solutions (corresponding to the values of t other than $0, 1, \ldots, d-1$) is congruent to some one of the integers in (i).

$x_1 + t_1\frac{m}{d} \equiv x_1 + t_2\frac{m}{d}$ (mod m), where $0 \leq t_1 < t_2 \leq d-1$ gives $t_1\frac{m}{d} \equiv t_2\frac{m}{d}$ (mod m)

$gcd(\frac{m}{d}, m) = \frac{m}{d} \Rightarrow t_1 \equiv t_2 \pmod{d} \Rightarrow d \mid t_2 - t_1$

This is an impossibility, because $0 < t_2 - t_1 < d$.

Thus all solutions in the list (i) are incongruent modulo m.

Let any other solution be $x_1 + t_j\frac{m}{d}$, where t_j is an integer other than $0, 1, \ldots, d-1$.

By Divison algorithm we can write $t_j = qd + r$, where q and r are integers and $0 \leq r \leq d-1$.

Then $x_1 + t_j\frac{m}{d} = x_1 + (qd + r)\frac{m}{d} \equiv x_1 + r\frac{m}{d}$(mod m).

Since $0 \leq r \leq d-1$, $x_1 + t_j\frac{m}{d}$ is one of the solutions listed in (i).

Thus the congruence $ax \equiv b$ (mod m) has d incongruent solutions listed in (i)

This completes the proof.

Note. The solutions belong to a single residue class modulo $\frac{m}{d}$ and this is the union of d distinct residue classes modulo m. The residue class $\bar{i}$ modulo $\frac{m}{d}$ is the union of d distinct residue classes $\bar{i}, \overline{i + \frac{m}{d}}, \overline{i + \frac{2m}{d}}, \ldots, \overline{i + \frac{(d-1)m}{d}}$ modulo m.

For example, the residue class $\bar{1}$ modulo 5 is the union of the three distinct residue classes $\bar{1}, \bar{6}, \overline{11}$ modulo 15.

Worked Examples.

1. Solve the linear congruence $5x \equiv 3$ (mod 11).

$gcd(5, 11) = 1$. Hence the congruence has a unique solution.

Since $gcd(5, 11) = 1$, there exist integers u, v such that $5u + 11v = 1$.

Here $u = -2, v = 1$. Therefore $5.(-2) + 11.1 = 1$ and this implies $5.(-2) \equiv 1$ (mod 11). Therefore $5.(-6) \equiv 3$ (mod 11).

Hence $x = -6$ is a solution.

All solutions are $x \equiv -6$ (mod 11), i.e., $x \equiv 5$ (mod 11).

All the solutions are congruent to 5 (mod 11) and therefore the given congruence has a unique solution.

2. Solve the linear congruence $15x \equiv 9 \pmod{18}$.

$gcd(15, 18) = 3$ and $3 \mid 9$. Therefore the given congruence has a solution. The given congruence is equivalent to $5x \equiv 3 \pmod{6}$.

$gcd(5, 6) = 1$. Hence the congruence $5x \equiv 3 \pmod{6}$ has a unique solution.

Since $gcd(5, 6) = 1$, there exist integers u, v such that $5u + 6v = 1$.

Here $u = -1. v = 1$. Therefore $5.(-1) + 6.1 = 1$ and this implies $5.(-1) \equiv 1(\mod 6)$. Therefore $5.(-3) \equiv 3 \pmod{6}$. Hence $x = -3$ is a solution of the congruence $5x \equiv 3 \pmod{6}$.

There are three incongruent solutions of the given congruence. They are $x = -3, -3 + 6, -3 + 12$ modulo 18, i.e., $x \equiv -3, 3, 9 \pmod{18}$.