UNIT 3: PRIMES AND THEIR DISTRIBUTION

UNIT STRUCTURE

3.1 Learning Objectives
3.2 Introduction
3.3 Prime numbers
3.4 Properties of Prime numbers
3.5 Fundamental Theorem of Arithmetic
3.6 Let Us Sum Up
3.7 Answers to Check Your Progress
3.8 Further Reading
3.9 Model Questions

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand the definition of prime numbers
- identifying prime and composite numbers
- exploring the significance of prime numbers in mathematics
- understand that every integer greater than 1 has a unique prime factorization
- apply prime factorization to solve problems
- recognize the significance of Fundamental Theorem of number theory

3.2 INTRODUCTION

Prime numbers are a fundamental concept in mathematics, particularly in number theory. A prime number is a natural number greater than 1 that has exactly two distinct factors 1 and itself. This means that a prime number cannot be divided evenly by any number other than 1 and itself. Examples of prime numbers include 2, 3, 5, 7, 11, 13, 17 and so on. Among these, 2 is the only even prime number.

In contrast, composite numbers are natural numbers greater than 1 that have more than two factors. For example, 6 is composite because it has factors 1, 2 , 3 and 6. The number 1 is a special case, it is neither prime nor composite because it has only one factor, itself.

Prime numbers play a significant role in various mathematical applications particularly in cryptography, coding theory, and computer algorithms. They are also used in solving problems related to divisibility, factorization and number patterns.

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be uniquely expressed as a product of prime numbers, except for the order of

multiplication. This theorem highlights the significance of prime numbers as the "building blocks" of all natural numbers.
For example,

$$30 = 2 \times 3 \times 5$$
$$60 = 2^2 \times 3 \times 5$$
$$84 = 2^2 \times 3 \times 7$$

The uniqueness of prime factorization means that no matter how we decompose a number into primes, the resulting prime numbers (when written in increasing order) will always be the same. This principle is fundamental in many areas of mathematics, including number theory, algebra, and cryptography.

Applications of Prime Numbers and the Fundamental Theorem of Arithmetic:

1. Finding the greatest common divisor (GCD) and least common multiple (LCM).
2. Prime numbers are widely used in encryption techniques such as RSA algorithm, which secures online communications, including banking transactions and data transfers.
3. Computer science and Algorithms: Many algorithms, including primality testing and integer factorization, rely on prime numbers for efficient computations.
4. Patterns in Number Theory: Prime numbers are studied for their unique properties and distributions, leading to deeper insights into the structure of numbers.

3.3 PRIME NUMBERS

Definition 3.3.1 (Prime Number) An integer $p > 1$ is called a prime number, or simply a prime, if its only positive divisors are 1 and p. An integer greater than 1 that is not prime is termed composite.

For example, 2, 3, 5, 7, 11, 13, 17, 19, ... are prime numbers, while 4, 6, 8, 9, 10, 12, 14, 15, ... are composite numbers. Note that the integer 2 is the only even prime and according to our definition the integer 1 plays a special role, being neither prime nor composite.

Definition 3.3.2 (Twin Prime) Two successive odd integers p and $p + 2$ which are prime are called twin prime. For example, 3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43 etc.

3.4 PROPERTIES OF PRIME NUMBERS

Theorem 3.4.1 If p is a prime and $p|ab$, then either $p|a$ or $p|b$.

Proof: If $p|a$, then there is nothing to prove. Assume $p \nmid a$. Then $\gcd(a, p) = 1$. By Euclid lemma, $p|b$.

Similarly, if $p \nmid b$, then we can prove $p|a$.

Hence if a prime $p|ab$, then either $p|a$ or $p|b$.

Corollary 3.4.2 If p is a prime and $p|a_1a_2a_3 \dots a_n$, then $p|a_k$ for some k, where $k = 1, 2, 3, \dots, n$.

Proof: We prove the result by induction on n, the number of factors. When $n = 1$, the result is obvious. When $n = 2$, the result is the content of theorem 3.4.1.

For $n > 2$, suppose whenever p divides a product of less than n factors, it divides at least one of the factors.

Let $p|a_1a_2 \dots a_n$. Then we can write

$$p|(a_1a_2 \dots a_{n-1})a_n$$

$$\Rightarrow p|a_1a_2 \dots a_{n-1} \text{ or } p|a_n, \text{ by theorem 3.4.1.}$$

If $p|a_n$, then there is nothing to prove. If $p|a_1a_2 \dots a_{n-1}$, then by induction hypothesis, $p|a_k$ for some k with $1 \leq k \leq n-1$.

Hence p divides one of the integers $a_1, a_2, \dots, a_n$.

Corollary 3.4.3 If $p, q_1, q_2, \dots, q_n$ are all primes and $p|q_1q_2 \dots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.

Proof: Let $p, q_1, q_2, \dots, q_n$ be all primes and

$$p|q_1q_2 \dots q_n$$

By corollary 3.4.2, $p|q_k$ for some k with $1 \leq k \leq n$. Since q_k is a prime number, q_k is divisible by 1 or q_k itself. Since $p > 1$, so $p = q_k$.

Theorem 3.4.4 Let $d > 1$ be the smallest positive divisor of an integer n. Then d is prime.

Proof: Let d_1 be any divisor of d. Then $1 \leq d_1 \leq d$.

Suppose $d_1 \neq 1$. Then $d_1|d$ and $d|n$

$$\Rightarrow d_1|n$$

Since d is the smallest divisor of n, so $d_1 \geq d$.

Hence $d_1 = d$. Since the only divisors of d are 1 and d iself. Hence d is prime.

Theorem 3.4.5 Prove that the product of twin prime numbers is one less than a perfect square.

Proof: Let p and $p + 2$ be two twin primes. Then $p, p + 1, p + 2$ are conjugate integers. So

$$(p+1)^2 = p(p+2)+1$$

$$\Rightarrow p(p+2) = (p+1)^2 - 1$$

Hence product of twin primes p and $p+2$ is one less of square of $(p+1)$.

W CHECK YOUR PROGRESS

Q 1. If $2^n - 1$ is prime number, then show that n is a prime number.

Q 2. If p and $p+2$ are twin primes and $p > 3$, then $p + (p+2)$ is divisible by 12.

Q 3. If $n > 2$, then prove that there exists a prime p such that $n < p < n!$.

Q 4. Show that every prime of the form $3k+1$ is also of the form $6m+1$.

Q 5. If a prime number $p > 3$, then show that $2p+1$ and $4p+1$ cannot be prime simultaneously.

Q 6. Prove that each integer of the form $3n+2$ has a prime factor.

Q 7. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.

Q 8. If p is prime and $p|a^n$, prove that $p^n|a^n$.

Q 9. Find all prime numbers that divides $50!$.

Q 10. If $p \geq q \geq 5$ and p and q are both primes, prove that $24|p^2 - q^2$.

Q 11. If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

3.5 FUNDAMENTAL THEOREM OF ARITHMETIC

Theorem 3.5.1 (Fundamental Theorem of Arithmetic or Unique Factorization Theorem) Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof: If n is prime number, then there is nothing to prove.

If n is a composite number, then there is at least an integer d such that $d|n, d > 1$. Let

$$S = \{d | d > 1, d|n, d \in Z\}$$

We have $n \in S \Rightarrow S \neq \phi$.

By well ordering principle, S has a least element, say p_i. Then $p_1 > 1$ and $p_1|n$. We have to prove p_1 is prime. If p_i is not prime, then p_1 has a divisor q such that $1 < q < p_1$ and $q|p_1$ and $1 < q < p_1$

$\Rightarrow q|n$ and $1 < q < p_1$

$\Rightarrow q \in S$ and $1 < q < p_1$

which is a contradiction to the fact that p_1 is the least element of S. Therefore p_1 is a prime number. Since $p_1|n$, therefore $\exists\ n_1 \in Z,\ 1 < n_1 < n$ and $n = p_1 n_1$ (1)

If n_1 is prime, then we have the required representation. If not, proceeding as above, we find another prime p_2 such that $n_1 = p_2 n_2$. $1 < n_2 < n_1$

From (1),

$$n = p_1 p_2 n_2 \qquad (2)$$

If n_2 is prime, then our proof is complete, otherwise there is a prime p_3 such that

$$n_2 = p_3 n_3, \quad 1 < n_3 < n_2 < n_1 < n$$

From (2),

$$n = p_1 p_2 p_3 n_3$$

The decreasing sequence $n > n_1 > n_2 > \cdots > 1$ cannot continue infinitely. So after a finite number of steps n_{k-1} must have a prime factor p_k (say). Thus we obtain

$$n = p_1 p_2 p_3 \ldots p_k$$

Uniqueness: Let us suppose that n can be represented as product of primes in two ways:

$$n = p_1 p_2 p_3 \ldots p_k = q_1 q_2 \ldots q_s \qquad (3)$$

where $k \leq s$ and p_i's and q_i's are primes written in increasing magnitude so that $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_s$.

Now

$$p_1 | n = q_1 q_2 \ldots q_s$$
$$\Rightarrow p_1 | q_j \quad for\ some \quad j = 1, 2, 3, \ldots, s$$
$$\Rightarrow p_1 = q_j \ \ as\ q_j\ is\ prime$$
$$\Rightarrow p_1 = q_j \geq q_1 \qquad (4)$$

Similarly, we can show that $q_1 \geq p_1 \qquad (5)$

From (4) and (5), we get $p_1 = q_1$

Cancelling the common factor in (3), we obtain

$$p_2 p_3 \ldots p_k = q_3 q_4 \ldots q_s$$

If $k < s$ and we continue the process, then we get

$$1 = q_{k+1} q_{k+2} \ldots q_s$$

which is absurd, because each $q_j > 1$. Hence $k = s$ and

$$p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$$

making the two factorization of n identitcal. The proof is now complete.

Of course, several of the primes that appear in the factorization of a given positive integer may be repeated, as in the case with $360 = 2.2.2.3.3.5$. By collecting like primes and replacing them by a single factor, we can rephrase Theorem 3.5.1 as a corollary.

Corollary 3.5.2 Any positive integer $n > 1$ can be written uniquely in a canonical form

$$n = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$$

where α_i is a positive integer for $i = 1, 2, \ldots, k$ and each p_i is prime such that

$$p_1 < p_2 < \cdots < p_k$$

Proof: By Fundamental Theorem of Arithmetic, we have

$$n = p_1 p_2 p_3 \ldots p_s \qquad (1)$$

In this decomposition primes $p_1, p_2, p_3, \ldots, p_s$ may be repeated. Combining the repeated factors of (1), we can write

$$n = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$$

where $p_1 < p_2 < \cdots < p_k$ and $\alpha_i \geq 1$.
Uniqueness can be proved as in the proof of Fundamental Theorem of Arithmetic.

Example 1: Represent 144 as the product of prime factors.
Solution: We have

$$144 \div 2 = 72$$
$$72 \div 2 = 36$$
$$36 \div 2 = 18$$
$$18 \div 2 = 9$$
$$9 \div 3 = 3$$

Therefore $144 = 2^4.3^2$

Example 2: Express 560 as the product of prime factors.
Solution: We have

$$560 \div 2 = 280$$
$$280 \div 2 = 140$$
$$140 \div 2 = 70$$
$$70 \div 2 = 35$$
$$35 \div 5 = 7$$

Therefore $560 = 2^4.5.7$

Theorem 3.5.3 If n is not divisible by any prime $\leq \sqrt{n}$, then n is a prime.
Proof: Suppose if possible n is not a prime. Then it is a composite number and so it can be written as

$$n = p_1^{\alpha_1}.p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$$
$$\geq p_1.p_2$$

Since n is not divisible by any prime $\leq \sqrt{n}$, so

$$p_1, p_2 > \sqrt{n}$$

Therefore

$$n \geq p_1.p_2 > \sqrt{n}\,.\sqrt{n}$$
$$\Rightarrow n > n$$

which is impossible. Hence n is prime.

Corollary 3.5.4 If n is a composite number, then the smallest prime divisor of n is less than or equal to $\sqrt{n}$.

Example 3: Show that 503 is a prime.
Solution: Since $2, 3, 5, 7, 11, 13, 17$ and 19 are the only primes $\leq \sqrt{503}$ and none of these primes divides 503, therefore 503 is a prime.

Theorem 3.5.5 (Euclid Theorem) There are infinite number of primes.
Proof: Suppose there are only finite number of primes $p_1, p_2, \ldots, p_r$ in ascending order.

Let $P = p_1.p_2.p_3 \ldots . p_r + 1$. Since $P > 1$, therefore by Fundamental Theorem of Arithmetic, there is some prime p such that $p|P$. But $p_1, p_2, \ldots p_r$ are the only prime numbers, so p must be equal to one of $p_1, p_2, \ldots, p_r$.
Thus

$$p|p_1.p_2 \ldots . p_r \quad and \quad p|P$$
$$\Rightarrow p|P - p_1.p_2 \ldots . p_r$$
$$\Rightarrow p|1$$

which contradicts the fact that $P > 1$.
Thus our assumption is wrong and hence there are infinite number of primes.
The above method of proof is interesting for, if we let $P_k = p_1 p_2 \ldots p_k + 1$, where $p_1, p_2, \ldots, p_k$ are the first k primes, then

$$P_1 = 2 + 1 = 3$$
$$P_2 = 2.3 + 1 = 7$$
$$P_3 = 2.3.5 + 1 = 31$$
$$P_4 = 2.3.5.7 + 1 = 211$$
$$P_5 = 2.3.5.7.11 + 1 = 2311$$

are all primes. This leads one to believe that
$P_k = 2.3 \ldots . p_k + 1$, where p_k is the kth prime, shall give all primes. But

$$P_6 = 2.3.5.7.11.13 + 1 = 30031 = 59.509$$
$$P_7 = 2.3.5.7.11.13.17 + 1 = 510511 = 19.97.277$$
$$P_8 = 2.3.5.7.11.13.17.19 + 1 = 9699691 = 347.27953$$

are all composite. A question whose answer is not known is whether there are infinite many primes p for which P_k is also prime.

At present, 22 primes of the form P_k has been identified.

Note: (1) Form the infinite sequence of positive integers

$$n_1 = 2$$
$$n_2 = n_1 + 1$$
$$n_3 = n_1 n_2 + 1$$
$$n_4 = n_1 n_2 n_3 + 1$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$n_k = n_1 n_2 n_3 \ldots n_{k-1} + 1$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots$$

since each $n_k > 1$, so each of these integers is divisible by a prime. But no two n_k can have same prime divisor. To prove this, let $\gcd(n_l, n_k) = d$, where $l < k$.
Then $d|n_l$ and hence $d|n_1 n_2 \ldots n_{k-1}$. Also $d|n_k$.
Therefore

$$d|n_k - n_1 n_2 \ldots n_{k-1}$$
$$\Rightarrow d|1$$
$$\Rightarrow d = 1$$

Hence the integers $n_k (k = 1, 2, \ldots)$ are pair wise relatively prime.

(2) Let p_n denote the nth of the prime numbers in their natural order. Euclid's proof shows that the expression $p_1p_2p_3 \dots p_n + 1$ is divisible by at least one prime. If there are several such prime divisors, then p_{n+1} cannot exceed the smallest of these so that

$$p_{n+1} \leq p_1p_2p_3 \dots p_n + 1 \quad for \ \ n \geq 1$$

Theorem 3.5.6 If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.

Proof: We prove the statement by induction on n.

Let $Q(n): p_n \leq 2^{2^{n-1}}$

For $n = 1, \ p_1 = 2 = 2^{2^{1-1}}$

Therefore $Q(1)$ is true.

Let $Q(k)$ is true for any positive integer k, i.e.

$$p_k \leq 2^{2^{k-1}}$$

We have to prove $Q(k+1)$ is true.

Now

$$\begin{aligned} p_{k+1} &\leq p_1p_2 \dots p_k + 1 \\ &\leq 2.2^2.2^{2^2} \dots p^{2^{k-1}} + 1 \\ &= 2^{(1+2+2^2+\cdots+2^{k-1})} + 1 \\ &= 2^{2^k-1} + 1 \end{aligned}$$

However, $1 \leq 2^{2^k-1}$ for all k; whence

$$\begin{aligned} p_{k+1} &\leq 2^{2^k-1} + 2^{2^k-1} \\ &= 2.2^{2^k-1} \\ &= 2^{2^k} \end{aligned}$$

Therefore $Q(k+1)$ is true. Hence by the principle of mathematical induction, $Q(n)$ is true for all $n \geq 1$, i.e.

$$p_n \leq 2^{2^{n-1}} \text{ for all } n \geq 1.$$

Corollary 3.5.7 For all $n \geq 1$, there are at least $n+1$ primes less than 2^{2^n}.

Proof: From theorem 3.5.6, $p_1, p_2, \dots, p_{n+1}$ are $n+1$ prime less than 2^{2^n}.

Theorem 3.5.8 There are infinitely many primes of the form $4n+3$.

Proof: If possible, we assume there exist finitely many primes of the form $4n+3$; call them $p_1, p_2, \dots p_k$. Consider the positive integer

$$\begin{aligned} m &= 4p_1p_2 \dots p_k - 1 \\ &= 4(p_1p_2 \dots p_k - 1) + 3 \end{aligned}$$

Clearly $m > 1$ and m is odd. Let $m = r_1.r_2 \dots .r_s$ be the prime factorization of m, where each $r_i (\neq 2)$ is a prime for $1 \leq i \leq s$. Since each r_i is odd, it is of the form $4n+1$ or $4n+3$. Since product of two or more integers of the form $4n+1$ is again an integer of the form $4n+1$. As m is of the form $4n+3$, it must have at least one prime factor r_i of the form $4n+3, 1 \leq i \leq s$. Let $r_i = p_j$ for some $j, 1 \leq j \leq k$.

Now $r_i|m$ and $r_i|p_j$

$\Rightarrow r_i|m$ and $r_i|4p_1p_2 \dots p_k$

$\Rightarrow r_i|1$

Which is a contradiction. Therefore our assumption is wrong. Hence there are infinitely many primes of the form $4n + 3$.

Theorem 3.5.9 There are infinitely many primes of the form $6k + 5$.
Proof: We observe that
(i) every prime > 3 is of the form $6q + 1$ or $6q + 5$ because the other possible form $6q, 6q + 2, 6q + 3, 6q + 4$ are not primes.
(ii) The product of two factors of the form $6q + 1$ is of the same form as shown below:
$(6q_1 + 1)(6q_2 + 1) = 6(6q_1q_2 + q_1 + q_2) + 1$
This shows that a number of the form $6k + 1$ need not be prime. Also product of two primes of the form $6q + 1$ is also of the for $6q + 1$. We have to prove there are infinitely many primes of the form $6k + 5$.

If possible, we assume there exist finitely many primes of the form $6k + 5$; call them $p_1, p_2, \dots p_n$. We consider the positive integer

$$N = 6p_1p_2p_3 \dots p_n - 1$$
$$= 6(p_1p_2p_3 \dots p_n - 1) + 5$$

Then clearly $N > 1$ and N is odd. Let $N = r_1.r_2 \dots .r_s$ be the prime factorization of N, where each $r_i(\neq 2)$ is a prime, $1 \leq i \leq s$. Since each r_i is odd, so it is of the form $6k + 1$. As N is of the form $6k + 5$, so it must have at least one prime factor, say r_i is of the form $6k + 5$. So

$$r_i = p_j \text{ for some } j,\ 1 \leq j \leq n$$

Now $r_i|N$ and $r_i|p_j$
$\Rightarrow r_i|N$ and $r_i|6p_1p_2p_3 \dots p_n$
$\Rightarrow r_i|1$
Which is a contradiction. Therefore, our assumption is wrong. Hence there are infinitely many primes of the form $6k + 5$.

W CHECK YOUR PROGRESS

Q 12. Find the prime factorization of the integers $1234, 10140$ and 36000.

Q 13. If $n > 1$ is an integer not of the form $6k + 3$, prove that of $n^2 + 2^n$ is composite.

Q 14. Prove that a positive integer $n > 1$ is a perfect square if and only if in the canonical form of n all the exponents of the primes are even integers.

Q 15. An integer is said to be square free if it is not divisible by the square of any integer greater than 1. Prove the following:

(a) A integer $n > 1$ is square free if and only if n can be factored into a product of distinct primes.

(b) Every integer $n > 1$ is the product of a square free integer and a perfect square.

Q 16. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

Q 17. Determine whether the integer 701 is prime by testing all prime $p \leq \sqrt{701}$ as possible divisors. Do the same for the integer 1009.

Q 18. Show that $\sqrt{p}$ is irrational for any prime p.

Q 19. Show that any composite three-digit number must have a prime factor less than or equal to 31.

Q 20. For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer that is greater than n.

Q 21. Assuming that p_n is the nth prime number, prove the following statements:

(a) $p_n > 2n - 1$ for $n \geq 5$

(b) None of the integers $P_n = p_1 p_2 \dots p_n + 1$ is a perfect square.

(c) The sum $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ is never an integer.

3.6 LET US SUM UP

- **Prime Number** An integer $p > 1$ is called a prime number, or simply a prime, if its only positive divisors are 1 and p. An integer greater than 1, that is not prime is termed composite.
- **Twin Prime** Two successive odd integers p and $p + 2$ which are prime are called twin primes.
- If p is a prime and $p|ab$, then either $p|a$ or $p|b$.
- If p is a prime and $p|a_1 a_2 a_3 \dots a_n$, then $p|a_k$ for some k, where $k = 1, 2, \dots, n$.
- If $p, q_1, q_2, \dots, q_n$ are all primes and $p|q_1 q_2 \dots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.
- Let $d > 1$ be the smallest positive divisor of an integer n. Then d is prime.
- Product of twin prime numbers is one less than a perfect square.
- **Fundamental Theorem of Arithmetic or Unique Factorization Theorem:** Every positive integer $n > 1$ is either a prime or a product of primes, this representation is unique, apart from the order in which the factors occurs.
- Any positive integer $n > 1$ can be written uniquely in a canonical form

$$n = p_1^{\alpha_1} . p_2^{\alpha_2} \dots . p_k^{\alpha_k}$$

where α_i is positive integer for $i = 1, 2, \dots, k$ and each p_i is prime such that $p_1 < p_2 < \cdots < p_k$.

- If n is not divisible by any prime $\leq \sqrt{n}$, then n is prime.

- If n is a composite number, then the smallest prime divisor of n is less than or equal to $\sqrt{n}$.
- If p_n is the nth prime number, then
$$p_n \leq 2^{2^{n-1}}$$
- For all $n \geq 1$, there are at least $n+1$ primes less than 2^{2^n}.
- There are infinite number of primes.
- There are infinitely many primes of the form $4n+3$.
- There are infinitely many primes of the form $6n+5$.

K 3.7 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q 1. Let $2^n - 1 = p$, a prime. We have to prove n is prime. If possible, let n be not a prime number. Then there exists positive integers r and s such that $n = rs$, where $1 < r, s < n$.
Therefore
$$\begin{aligned} p &= 2^n - 1 \\ &= 2^{rs} - 1 \\ &(2^r)^s - 1 \\ &= x^s - 1, \text{ where } x = 2^r > 2 \text{ for } r > 1 \\ &= (x-1)(x^{s-1} + x^{s-2} + \cdots + x + 1) \end{aligned}$$
which implies either $x - 1 = 1$ or $x^{s-1} + x^{s-2} + \cdots + x + 1 = 1$
$$x = 2 \text{ or } x^{s-1} + x^{s-2} + \cdots + x = 0$$
$x = 2$ and $x^{s-1} + x^{s-2} + \cdots + x = 0$ are both not true.
Thus, our assumption is wrong. Hence n is prime.

Answer to Q 2. Let $p(>3)$ and $p+2$ be two twin prime. Then by division algorithm, p is of the form $6k+1$ or $6k+5$.
If $p = 6k+1$, then $p + 2 = 6k + 3 = 3(2k+1)$, which is not prime. Since p and $p+2$ are twin prime number, so p is not of the form $6k+1$. Therefore p is of the form $p = 6k+5$.
Now
$$\begin{aligned} p + (p+2) &= (6k+5) + (6k+5+2) \\ &= 12k + 12 \\ &= 12(k+1) \end{aligned}$$
which is divisible by 12.

Answer to Q 3. Let us consider the integer $n! - 1$. If $n! - 1$ is a prime number, say p, i.e. $p = n! - 1$, then $p < n!$.
For $n > 2$,
$$n! - 1 > n$$

$$\Rightarrow p > n$$

Therefore $n < p < n!$

For $n > 2,\ n! - 1 > 1$. If $n! - 1$ is not prime, then by Fundamental Theorem of Arithmetic, there exists a prime p such that

$$p|n! - 1$$
$$\Rightarrow p \leq n! - 1$$
$$\Rightarrow p < n!$$

Finally, we have to prove $p > n$. If possible, suppose $p \leq n$. Then $p|n!$.

Now $p|n!$ and $p|n! - 1$

$\Rightarrow p|n! - (n! - 1)$

$\Rightarrow p|1$, a contradiction. This contradiction implies that $p > n$. Hence $n < p < n!$

Answer to Q 4. Let $n = 3m + 1$ be a prime number for any positive integer m. Now m may be even or odd, i.e., $m = 2k$ or $m = 2k + 1$.

If $m = 2k$, then $n = 3m + 1 = 3.2k + 1 = 6k + 1$

If $m = 2k + 1$, then $n = 3(2k + 1) + 1 = 6k + 4 = 2(3k + 2)$

which is not a prime. Therefore prime n of the form $3m + 1$ will also be of the form $6k + 1$.

Answer to Q 5. Since p is a prime greater than 3, p is either of the form $6k + 1$ or $6k + 5$.

If $p = 6k + 1$, then $2p + 1 = 2(6k + 1) + 1 = 12k + 3 = 3(4k + 1)$

i.e., $2p + 1$ is not prime.

$$4p + 1 = 4(6k + 1) + 1 = 24k + 5 = 6.(4k) + 5$$

which is of the form $6k + 5$.

If $p = 6k + 5$, then $2p + 1 = 2(6k + 5) + 1 = 12k + 11 = 12k + 6 + 5 = 6(2k + 1) + 5$

which is of the form $6k + 5$.

$$4p + 1 = 4.(6k + 5) + 1$$
$$= 24k + 21$$
$$= 3(8k + 7)$$

i.e., 4p+1 is not prime.

Hence for any prime $p > 3$, $2p + 1$ and $4p + 1$ cannot be prime simultaneously.

Answer to Q 6. Let p be any prime factor of $3n + 2$. Then p is of the form $3k + 1$ or $3k + 2$, by division algorithm.

If all prime factor of $3n + 2$ is of the form $3k + 1$ then $3n + 2$ will be of the form $3k + 1$, which is not possible.

Hence every integer of the form $3n + 2$ has a prime factor of that form.

Answer to Q 7. Since $p \geq 5$, therefore p is of the form $6k + 1$ or $6k + 5$.

If $p = 6k + 1$, then $p^2 + 2 = (6k + 1)^2 + 2 = 36k^2 + 12k + 3 = 3(12k^2 + 4k + 1)$

If $p = 6k + 5$, then $p^2 + 2 = (6k + 5)^2 + 2 = 36k^2 + 6k + 27 = 3(12k^2 + 2k + 9)$

In either case, $3|p^2 + 2$, so $p^2 + 2$ is composite.

Answer to Q 8. Let p be prime and $p|a^n$.
By corollary 3.4.2, $p|a \Rightarrow a = pk$, for some k
Therefore

$$a^n = p^n k^n$$
$$\Rightarrow p^n | a^n$$

Answer to Q 9. Since each prime number less than 50 is a factor of $50!$, so all prime less than 50 will divide $50!$.

By Fundamental Theorem of Arithmetic, each factor k of $50!$ that is non-prime has a unique prime factorization and each factor of the unique factorization of k is smaller than k and so is a prime that is less than 50. Thus, there is no prime $>$ 50 present in the factorization of k. Hence all prime < 50 divides $50!$.

Answer to Q 10. Since $p \geq q \geq 5$ and p, q primes, therefore both are of the form $6k + 1$ or $6k + 5$.
We have following 4 possibilities:
(i) $p = 6k + 1,\ q = 6k + 1$
(ii) $p = 6k + 1,\ q = 6k + 5$
(iii) $p = 6k + 5,\ q = 6k + 1$
(iv) $p = 6k + 5,\ q = 6k + 5$
The situations (ii) and (iii) are equivalent.
Case-I Let $p = 6r + 1,\ q = 6s + 1$, where $r, s > 0$. Then

$$p^2 - q^2 = (p + q)(p - q)$$
$$= (6r + 6s + 2)(6r - 6s)$$
$$= 12(3r + 3s + 1)(r - s)$$

If r and s are both even or both odd, then $r - s$ is even and $\neq 0$. Let $r - s = 2k$.
Then

$$p^2 - q^2 = 12(3r + 3s + 1).2k$$
$$= 24(3r + 3s + 1).k$$
$$\Rightarrow 24|p^2 - q^2$$

If one of r and s is even and other is odd, then $3r + 3s + 1$ is even. Let $3r + 3s + 1 = 2k$. Then

$$p^2 - q^2 = 12.2k(r - s)$$
$$= 24k(r - s)$$
$$\Rightarrow 24|p^2 - q^2$$

Case-II Let $p = 6r + 1,\ q = 6s + 5\ (r > 0, s \geq 0)$. Then

$$p^2 - q^2 = (p + q)(p - q)$$
$$= (6r + 6s + 6)(6r - 6s - 4)$$
$$= 12(r + s + 1)(3r - 3s - 2)$$

If one of r and s is even and other is odd, then $r + s + 1$ is even. Let $r + s + 1 = 2k$. Then

$$p^2 - q^2 = 12(r + s + 1).2k$$
$$= 24|(r + s + 1)k$$

$$24|p^2 - q^2$$

Case-III Let $p = 6r + 5,\ q = 6s + 5\ \ (r, s \geq 0)$. Then

$$p^2 - q^2 = (p + q)(p - q)$$
$$= (6r + 6s + 10)(6r - 6s)$$
$$= 12(3r + 3s + 5)(r - s)$$

If r and s are both even or both odd, then $r - s$ is even. Let $r - s = 2k$. Then

$$p^2 - q^2 = 12(3r + 3s + 5).2k$$
$$= 24(3r + 3s + 5)k$$
$$24|p^2 - q^2$$

If one of r and s is even and other is odd, then $3r + 3s + 5$ is even. Let $3r + 3s + 5 = 2k$. Then

$$p^2 - q^2 = 24k(r - s)$$
$$\Rightarrow 24|p^2 - q^2$$

Hence from above, we can conclude that for $p \geq q \geq 5$ and p, q primes, $24|p^2 - q^2$.

Answer to Q 11. Let $p(\neq 5)$ be an odd prime. Then p is of the form $10k + 1, 10k + 7$ and $10k + 9$, since $10k +$ even number can factor out 2.

If $p = 10k + 1$, then $p^2 - 1 = (10k + 1)^2 - 1 = 10(10k^2 + 2k)$

$$\Rightarrow 10|p^2 - 1$$

If $p = 10k + 3$, then $p^2 + 1 = (10k + 3)^2 + 1 = 10(10k^2 + 6k + 1)$

$$10|p^2 + 1$$

If $p = 10k + 7$, then $p^2 + 1 = (10k + 7)^2 + 1 = 10(10k^2 + 14k + 5)$

$$\Rightarrow 10|p^2 + 1$$

If $p = 10k + 9$, then $p^2 - 1 = (10k + 9)^2 - 1 = 10(10k^2 + 18k + 8)$

$$\Rightarrow 10|p^2 - 1$$

Hence if $p(\neq 5)$ is an odd prime, then either $10|p^2 - 1$ or $10|p^2 + 1$.

Answer to Q 12. Left as an exercise.

Answer to Q 13. Let $n > 1$ be an integer not of the form $6k + 3$. Then n is of the form $6k, 6k + 1, 6k + 2, 6k + 4, 6k + 5$.

If $n = 6k, n^2 + 2^n = 36k^2 + 2^{6k} \Rightarrow 2|n^2 + 2^n$

If $n = 6k + 1$, then

$$n^2 + 2^n = (6k + 1)^2 + 2^{6k+1}$$
$$= 36k^2 + 12k + 1 + 2^{6k+1}$$
$$= 36k^2 + 12k + \left(1^{6k+1} + 2^{6k+1}\right)$$
$$= 36k^2 + 12k + (1 + 2)\left(1 - 2 + 2^2 - \cdots + 2^{6k}\right)$$
$$= 3\left\{12k^2 + 4k + \left(2^{6k} - \cdots + 2^2 - 2 + 1\right)\right\}$$
$$\Rightarrow 3|n^2 + 2^n$$

If $n = 6k + 2$, then

$$n^2 + 2^n = (6k + 2)^2 + 2^{6k+2}$$
$$= 36k^2 + 24k + 4 + 2.2^{6k}$$
$$= 2\left(18k^2 + 12k + 2 + 2^{6k}\right)$$
$$\Rightarrow 2|n^2 + 2^n$$

Similarly, we can show if $n = 6k + 4$, then $2|n^2 + 2^n$.
If $n = 6k + 5$, then

$$\begin{aligned} n^2 + 2^n &= (6k+5)^2 + 2^{6k+5} \\ &= 36k^2 + 60k + 25 + 2^{6k+5} \\ &= 36k^2 + 60k + 24 + \left(1 + 2^{6k+5}\right) \\ &= 36k^2 + 60k + 24 + (1+2)\left(1 - 2 + 2^2 - \cdots + 2^{6k+4}\right) \\ &= 3\left\{12k^2 + 20k + 8 + \left(1 - 2 + 2^2 - \cdots + 2^{6k+4}\right)\right\} \\ &\Rightarrow 3|n^2 + 2^n \end{aligned}$$

Hence if $n > 1$ is an integer not of the form $6k + 3$, $n^2 + 2^n$ is composite.

Answer to Q 14. Left as an exercise.

Answer to Q 15. (a) Suppose n is square free and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ be the prime factorization.

Suppose any $\alpha_i > 1$. If $\alpha_i \geq 2$, then p_i^2 will divide n. Which is a contradiction to the fact that n is square free. Hence each $\alpha_i = 1$, i.e., n is product of distinct primes.

Conversely, suppose n can be factored into a product of distinct primes, i.e. $n = p_1 p_2 \dots p_r$ where $p_i \neq \alpha_j$ for $i \neq j$. We have to prove n is square free. If possible, suppose n is not square free. Let

$$a^2|n$$

$n = a^2 x$ for some integer x
$\Rightarrow p_1 p_2 \dots p_r = x q_1^{2k_1} . q_2^{2k_2} \dots . q_s^{2k_s}$, where $a^2 = q_1^{2k_1} . q_2^{2k_2} \dots . q_s^{2k_s}$
$\Rightarrow q_i | p_1 p_2 \dots p_r$ for $i = 1, 2, \dots, s$
$\Rightarrow q_i = p_l$ for some $l,\ 1 \leq l \leq r$
After factoring out q_i and p_l, we still have

$$p_1 p_2 \dots p_{l-1} p_{l+1} \dots p_r = x q_1^{2k_1} . q_2^{2k_2} \dots q_i^{2k_i - 1} \dots . q_s^{2k_s}$$

so that
$q_i | p_1 p_2 \dots p_{l-1} p_{l+1} \dots p_r$. But original factorization $p_1 p_2 \dots p_r$ was unique and $q_i = p_l$ was factored out. Therefore q_i cannot divide the remaining factorization. Hence n must be square free.

(b) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ be the canonical form. If α_i is odd and $\alpha_i > 1$, then $\alpha_i - 1$ is even. Let

$$a = p_{r_1}^{\alpha_{r_1}} . p_{r_2}^{\alpha_{r_2}} \dots . p_{r_m}^{\alpha_{r_m}}$$

where $1 \leq r_i \leq s$ and α_{r_i} is odd and $\alpha_{r_i} \geq 1$. Consider $b = p_{r_1} . p_{r_2} \dots . p_{r_m}$. Then $a = b p_{r_1}^{\alpha_{r_1} - 1} . p_{r_2}^{\alpha_{r_2} - 1} \dots . p_{r_m}^{\alpha_{r_m} - 1}$. Also b is square free by part (a) and $p_{r_i}^{\alpha_{r_i} - 1} = p_{r_i}^{2x_i}$ since $\alpha_{r_i} - 1$ is even.
Let $c = p_{r_1}^{x_1} p_{r_2}^{x_2} \dots p_{r_m}^{x_m}$. Then $a = bc^2$.

Finally, let $\frac{n}{a} = p_{t_1}^{\alpha_{t_1}} \dots p_{t_j}^{\alpha_{t_j}}$, where all α_{t_i} are even since $\frac{n}{a}$ has factored out all of the odd exponents in the canonical form of n. Therefore

$$\frac{n}{a} = d^2$$
$$\Rightarrow n = ad^2$$
$$= bc^2d^2$$
$$= b(cd)^2, \text{ where } b \text{ is square free.}$$

Answer to Q 16. Assume $n > 0$. We have to show $n = 2^k m$, where $k \geq 0$ and m is odd.
If n is odd, choose $k = 0$ and $m = n$.
If n is even, then $n = 2l_1$, where $l_1 < n$. If l_1 is odd, choose $k = 1$ and $m = l_1$. If l_1 is even, then $l_1 = 2l_2$, so $n = 2^2 l_2$. Note $l_2 < l_1$. Continue this process till l_1 is odd. Then $m = l_i$ and $k = i$. Since $l_{i+1} < l_i$, this is a finite process.

Answer to Q 17. Left as an exercise.

Answer to Q 18. Left as an exercise.

Answer to Q 19. Since 999 is the largest 3-digit number and $\sqrt{999} = 31.6$ ..., since 999 is a composite number, sp it has a prime factor less than or equal $\sqrt{999} = 31.6$. Also from Theorem 3.5.3, any composite 3-digit number must have a prime factor ≤ 31.

Answer to Q 20. Since $n!$ is even as it contains 2, therefore $n! + 1$ is odd and hence every prime divisor of $n! + 1$ is odd. We have to prove these prime divisors are greater than n.
If possible, let every prime divisor p_i of $n! + 1$ is such that $p_i \leq n$. Let $p = n! + 1$.
Clearly $p_i | n!$, since p_i is one of the members of $n!$.
Therefore, we have
$p_i | p$ and $p_i | n!$
$\Rightarrow p_i | p - n!$
$\Rightarrow p_i | 1$, a contradiction.
Therefore, our assumption $p_i \leq n$ is wrong. Hence $p_i > n$.

Answer to Q 21. (a) We prove the result by induction on n. Let

$$Q(n): p_n > 2n - 1$$

For $n = 5,\ p_n = p_5 = 11 > 2.5 - 1$
i.e. $Q(5)$ is true.
We assume $Q(k)$ is true for any integer > 5, i.e.

$$p_k > 2k - 1$$

$\Rightarrow p_k + 2 > (2k - 1) + 2$ [since $p_k + 1$ is even, so the next possible prime is $p_k + 2$]

$$\Rightarrow p_{k+1} > p_k + 2 > 2(k + 1) - 1$$

Thus $Q(k+1)$ is true. Hence by the principle of mathematical induction, $Q(n)$ is true for $n \geq 5$.

(b) Since $p_1 = 2$, so $p_1 p_2 \ldots p_n$ is even.
$\Rightarrow p_1 p_2 p_3 \ldots p_n + 1$ is odd
$\Rightarrow p_n$ is odd.
By division algorithm, $p_n = 4k + r,\ r = 0, 1, 2, 3$
But p_n is odd, so $r = 1, 3$
If $r = 1$, then $p_1 p_2 p_3 \ldots p_n + 1 = 4k + 1$

$$\Rightarrow p_1 p_2 p_3 \ldots p_n = 4k$$
$$\Rightarrow p_2 p_3 \ldots p_n = 2k \ \ as \ \ p_1 = 2$$

Since $p_2, p_3, \ldots, p_n$ are all odd prime, so their product is also odd. But $2k$ is even. Therefore $r \neq 1$. Thus $p_n = 4k + 3$ for all n. We have to prove p^n is not perfect square. If possible, let $p_n = s^2$, for some integer s, Then $s^2 = 4k + 3$.

Since s^2 is odd, so is s. Let $s = 2a + 1$, for some integer a.

Therefore

$$s^2 = 4k + 3$$
$$\Rightarrow (2a+1)^2 = 4k + 3$$
$$\Rightarrow 4a^2 + 4a + 1 = 4k + 3$$
$$\Rightarrow 4a^2 + 4a = 4k + 2$$
$$2a^2 + 2a = 2k + 1$$

which shows that a even number is equal to a odd number. Which is impossible. Hence there is no s such that $p_n = s^2$.

(c) Let $P = p_1 p_2 \ldots p_n$ and suppose $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} = a$, for some integer a. Then

$$\frac{P}{p_1} + \frac{P}{p_2} + \cdots + \frac{P}{p_n} = aP$$

Since $p_1 | aP$, therefore $p_1 | \frac{P}{p_1}$, $p_1 | \frac{P}{p_2}$, ... , $p_1 | \frac{P}{p_n}$
$\Rightarrow p_1 | p_2 p_3 \ldots p_n$, which is a contradiction.
Therefore, our assumption $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ = a integer is wrong.
Hence $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ is never an integer.

O 3.8 FURTHER READING

1. David M. Burton, Elementary Number Theory (7th Edn.), McGraw Hill Education (India) Private Limited, Chennai-60016, 2018.

2. S.B. Malik, Basic Number Theory (2nd revised Edn.), Vikas Publishing House Private Limited, Noida-201301, 2017.

3. H. Kishan, Number Theory, Krishna Prakashan Media (P) Ltd., Meerut-250001 (UP), India, 2017.

4. George E. Andrews, Number Theory, Hindustan Publishing Corporation, New Delhi.

5. Hardy, G.H. and Wright, E.M., Theory of Numbers, Oxford Science Publications, 2003.

M 3.9 MODEL QUESTIONS

1. Find the prime power factorizations of $132,400$ and 1995. Hence find $\gcd(132,400), \gcd(400,1995), \gcd(400,132,1995)$.
2. If a positive integer m is not a perfect square, then prove that $\sqrt{m}$ is irrational.
3. If a and b are two odd integers, then show that a^2+b^2 cannot be a perfect square.
4. Prove that n^4+4^n is composite for all integers $n>1$.
5. Show that 1949 and 1951 are twin primes.
6. Determine whther the integer 701 is prime by testing all primes $p \le \sqrt{701}$ as possible divisors.
7. Show that 2093 is not a prime.
8. If $n>1$, show that $n!$ is never a perfect square.
9. If $\gcd(a,b)=p$, a prime, what are the possible values of $\gcd(a^2,b^2), \gcd(a^2,b)$ and $\gcd(a^3,b^2)$?
10. Any integer of the form 8^n+1, where $n \ge 1$, is composite.
11. For the repunits $R_n = 111\ldots1$(n-times) (e.g. $R_2=11, R_3=111$), verify the followings:

(a) If $n|m$, then $R_n|R_m$

(b) If $d|R_n$ and $d|R_m$, then $d|R_{n+m}$

(c) If $\gcd(n,m)=1$, then $\gcd(R_n,R_m)=1$.

*** *** ***