Unit 2: DIVISIBILITY THEORY

UNIT STRUCTURE

2.1 Learning Objectives
2.2 Introduction
2.3 Divisibility
2.4 Properties of Divisibility
2.5 Tests of Divisibility
2.6 Let Us Sum Up
2.7 Answers to Check Your Progress
2.8 Further Reading
2.9 Model Questions

2.1 LEARNING OBJECTIVES

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

- Understand basic concepts.
- Identify and apply divisibility rules for common integers like 2, 3, 5, 10 etc.
- Practice using these rules to quickly check divisibility.
- Know the properties of divisibility.
- Develop logical reasoning to prove divisibility statements.

2.2 INTRODUCTION

Divisibility theory is a fundamental concept in the study of number theory, which is a branch of pure mathematics dedicated to understanding the properties and relationships of integers. Divisibility concerns the conditions under which one integer can be evenly divided by another without learning a remainder. It forms the basis for many advanced mathematical ideas, including prime factorization, the greatest common divisor (GCD), least common multiple (LCM), modular arithmetic and even cryptography.

Understanding divisibility is essential because it helps in simplifying complex mathematical problems, identifying patterns and solving real life challenges involving distribution, arrangement and computation. This introduction explores the basic concepts, properties and applications of divisibility theory, providing a comprehensive foundation for deeper mathematical studies.

Basic Concepts of Divisibility

In mathematics, an integer a is said to be divisible by another integer b if after dividing a by b, the result is an integer with zero remainder. Mathematically, this relationship is expressed using the notation $b|a$, which read as "b divides a". For example, 12 is divisible by 3 because dividing 12 by 3 results in the integer 4, with no remainder. 13 is not divisible by 3 because the division leaves a remainder of 1.

This concept can also be expressed using the equation:

$$a = bq$$

Where a is the dividend, b is the divisor, q is the quotient and the remainder is zero.

Divisibility is one of the earliest mathematical concepts taught in elementary mathematics and it forms the groundwork for more advanced mathematical reasoning and problem solving.

Divisibility Rules

To simplify the process of checking whether one number divides another, mathematicians have developed divisibility rules. These are simple guidelines that help determine divisibility without performing long division. These rules are especially useful for quickly determining divisibility in mental math and solving mathematical problems involving large numbers.

Prime and Composite Numbers

Divisibility theory is closely related to the concepts of prime and composite numbers.

A prime number is an integer greater than 1 that has exactly two distinct positive divisors 1 and itself. For example, $2, 3, 5, 7, 11$ and so on.

A composite number is an integer greater than 1 that has more than two distinct divisors. For example, $4, 6, 8, 9, 10$ and so on.

Understanding prime numbers is crucial in divisibility theory because every positive integer greater than 1 can be uniquely expressed as a product of prime numbers. This is known as the Fundamental Theorem of Arithmetic and it serves as a cornerstone in the study of divisibility and number theory.

Greatest Common Divisor (GCD) and Least Common Multiple (LCM)

Two key concepts derived from divisibility are the greatest common divisor (gcd) and least common multiple (lcm). There are several methods for calculating GCD and LCM:

(i) Prime Factorization: Listing the prime factors of each number and using them to determine the GCD and LCM.

(ii) Euclidean Algorithm: A systematic method for finding the GCD using repeated division.

(iii) Division Method: Dividing the numbers by their common prime factors to determine the LCM.

Understanding how to calculate GCD and LCM is essential for solving problems involving ratios, fractions and algebraic equations.

The properties of divisibility are fundamental when solving complex divisibility problems, proving mathematical statements and simplifying algebraic expressions.

Applications of Divisibility Theory

Divisibility theory has broad applications in both mathematics and real-life problem-solving. Some notable applications include:

1. **Simplifying Fractions:** By finding the GCD of the numerator and denominator, fractions can be reduced to their simplest forms.

2. **Solving Word Problems:** Divisibility helps in solving problems related to grouping, arranging and distributing items evenly.

3. **Cryptography:** Modern cryptographic systems, such as RSA, use prime factorization and divisibility principles to ensure data security.

4. **Mathematical Proofs:** Divisibility concepts are used in constructing and understanding mathematical proofs, especially in number theory.

5. **Programming Algorithms:** Divisibility algorithms are used in software development for tasks like error detection, data validation and optimization

6. **Modular Arithmetic and Divisibility:** Modular arithmetic also known as "clock arithmetic", is another concept that arises from divisibility. It deals with integers and their remainders when divided by a given number (called the modulus). For example, in modulo 5, the number 7 is congruent to 2 because 7 divided by 5 leaves a remainder of 2, denoted as

$$7 \equiv 2 \ (mod \ 5)$$

Modular arithmetic has practical applications in areas like computer science, cryptography and number theory. It simplifies problems involving divisibility cyclic patterns.

7. **Real-Life Scenarios:** Divisibility helps in situations like creating schedules, determining cycles and calculating frequencies in scientific research.

2.3 DIVISIBILITY

Definition 2.3.1 An integer b is said to be divisible by an integer $a \neq 0$, in symbols $a|b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

For example, -15 is divisible by 5 because $-15 = 5.(-3)$. However 18 is not divisible by 5; for there is no integer c that amkes the statement $18 = 5c$ true. $a|b$ is also read as 'a is divisor of b' or 'a is factor of b' or 'b is multiple of a'.

If a is a divisor of b, then b is also divisible by $-a$ because $b = ac$ we can write $b = (-a)(-c)$. Therefore the divisors of an integer always occur in pairs. To find all the divisors of a given integers, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers.

2.4 PROPERTIES OF DIVISIBILITY

Theorem 2.4.1 For integers a, b, c, the following hold:

(a) $a|0, 1|a, a|a$.

(b) $a|1$ if and only if $a = \pm 1$.

(c) If $a|b$ and $c|d$, then $ac|bd$

(d) If $a|b$ and $b|c$, then $a|c$.

(e) $a|b$ and $b|a$ if and only if $a = \pm b$.

(f) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

(g) If $a|b$ and $a|c$, then $a|bx + cy$ for arbitrary integers x and y.

Proof: (a) For any integer a, we can write

$$0 = a.0$$

which implies $$a|0$$

$$a = a.1$$

$$\Rightarrow 1|a \text{ and } a|a.$$

(b) Let $a|1$. Then $1 = a.c$ for some integer c.

Which is possible only if $a = 1$ and $c = 1$

or $a = -1$ and $c = -1$

i.e. if $a = \pm 1$

Conversely, let $a = \pm 1$. Then obviously $a|1$, because $1 = 1.1$ and $1 = (-1)(-1)$.

(c) Let $a|b$ and $c|d$. Then there exist integers r, s such that $b = ar$ and $d = cs$ so that

$$bd = ar.cs$$

$$= (rs).(ac)$$

$$\Rightarrow ac|bd$$

(d) Let $a|b$ and $b|c$. Then there exist $r, s \in Z$ such that $b = ar$ and $c = bs$ so that

$$c = bs$$

$$= (ar)s$$

$$= a(rs)$$

Therefore $a|c$.

(e) Let $a|b$ and $b|a$. Then there exist integers r, s such that $b = ar$ and $a = bs$. Then

$$b = (bs)r$$
$$\Rightarrow b = b(rs)$$
$$\Rightarrow rs = 1$$
$$\Rightarrow r = 1, s = 1 \text{ or } r = -1, s = -1$$

If $s = 1$, then $a = b$ and if $s = -1$, then $a = -b$.

Thus $a = \pm b$.

Conversely, let $a = \pm b$. We have to prove $a|b$ and $b|a$.

If $a = b$, then $a|b$ and $b|a$.

Also, if $a = -b$, then $a|b$ and $b|a$.

(f) Let $a|b$ and $b \neq 0$. For $a|b$ there exists an integer c such that $b = ac$. Since $b \neq 0$.

For $a|b$ there exists an integer c such that $b = ac$. Since $b \neq 0$, therefore $c \neq 0$. Now

$$|b| = |ac| = |a||c|$$

Since $c \neq 0$, so it follows that $|c| \geq 1$. Therefore

$$|b| = |a||c| \geq |a|$$

(g) Let $a|b$ and $a|c$. Then there exist integers r and s such that $b = ar$ and $c = as$. But for arbitrary integers x and y,

$$bx + cy = arx + asy$$
$$= a(rx + sy)$$
$$\Rightarrow a|bx + cy \text{ as } rx + sy \text{ is an integer.}$$

Example 1: If $a|b$, show that $(-a)|b, a|(-b)$ and $(-a)|(-b)$.

Solution: Let $a|b$. Then there exists $c \in Z$ such that $b = ac$

So we write

$$b = ac = (-a)(-c) \Rightarrow -a|b$$
$$-b = -ac = a.(-c) \Rightarrow a|(-b)$$
$$-b = -ac = (-a).c \Rightarrow (-a)|(-b)$$

Example 2: Given integers $a, b, c, d,$ verify the following:

(a) If $a|b$, then $a|bc$

(b) If $a|b$ and $a|c$, then $a^2|bc$

(c) $a|b$ if and only if $ac|bc$, where $c \neq 0$.

Solution: (a) Let $a|b$. Then there exists an integer x such that $b = ax$.

Now

$$bc = ax.c = a(xc)$$
$$\Rightarrow a|bc$$

(b) Let $a|b$ and $a|c$. Then there exist $x, y \in Z$ such that $b = ax, c = ay$.

Now

$$bc = (ax)(ay) = a^2(xy)$$
$$\Rightarrow a^2|bc$$

(c) Let $a|b$. Then there exists an integer x such that $b = ax$.

Now

$$bc = ax.c$$
$$= (ac)x$$
$$\Rightarrow ac|bc$$

Conversely, let $ac|bc, c \neq 0$. Then there exists integer y such that

$$bc = (ac)y$$
$$\Rightarrow b = ay \quad [\text{since } c \neq 0]$$
$$\Rightarrow a|b$$

Example 3: Prove or disprove: If $a|b + c$, then either $a|b$ or $a|c$.

Solution: Not true.

Let $a = 3, b = 2, c = 7$. Then $a = 3|2 + 7 = b + c$ but $a = 3 \nmid 2 = b, a = 3 \nmid 7 = c$.

Example 4: For $n \geq 1$, use mathematical induction to establish each of the following divisibility statements:

(a) $8|5^{2n} + 7$

(b) $15|2^{4n} - 1$

Solution: (a) Let

$$P(n): 8|5^{2n} + 7$$

For $n = 1, 5^{2.1} + 7 = 32$, which is divisible by 8.

i.e. $P(n)$ is true for $n = 1$.

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

$$8|5^{2k} + 7$$
$$\Rightarrow \text{there exists } x \in Z \text{ such that } 5^{2k} + 7 = 8x \qquad (*)$$

Now we have to prove $P(k + 1)$ is true.

$$5^{2(k+1)} + 7 = 5^2.5^{2k} + 7$$
$$= 5^2.(8x - 7) + 7 \qquad [\text{using } (*)]$$
$$= 200x - 168$$

$$= 8(25x - 21)$$
$$\Rightarrow 8|5^{2(k+1)} + 7$$

Therefore $P(k+1)$ is true. Hence by mathematical induction $P(n)$ is true for all $n \in N$, i.e. $8|5^{2n} + 7$ for all $n \geq 1$.

(b) Let $P(n): 15|2^{4n} - 1$

For $n = 1, 2^{4.1} - 1 = 15$, which is divisible by 15.

Therefore $P(1)$ is true.

We assume $P(k)$ is true for any positive integer k,

i.e.

$$15|2^{4k} - 1$$
$$\Rightarrow 2^{4k} - 1 = 15x$$
$$\Rightarrow 2^{4k} = 15x + 1 \qquad (*)$$

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

Now

$$2^{4(k+1)} - 1 = 2^{4k}.2^4 - 1$$
$$= (15x + 1).16 - 1 \qquad \text{[using } (*)\text{]}$$
$$= 15.16x + 15$$
$$= 15(16x + 1)$$
$$\Rightarrow 15|2^{4(k+1)} - 1$$

Therefore $P(k+1)$ is true.

Hence by mathematical induction, the given statement $P(n)$ is true for all $n \geq 1$, i.e.

$$15|2^{4n} - 1 \text{ for all } n \geq 1.$$

Example 5: For an arbitrary integer a, verify the following:

(a) $2|a(a+1)$ and $3|a(a+1)(a+2)$

(b) $3|a(2a^2 + 7)$

Solution: Since a is an arbitrary integer, therefore by division algorithm a is of the forms: $2q$ or $2q+1$.

If $a = 2q$, then

$$a(a+1) = 2q(2q+1)$$
$$\Rightarrow 2|a(a+1)$$

If $a = 2q+1$, then

$$a(a+1) = (2q+1)(2q+1+1)$$
$$= (2q+1)(2q+2)$$

$$= 2(2q+1)(q+1)$$
$$\Rightarrow 2|a(a+1)$$

2nd Part: Since a is an arbitrary integer, therefore by division algorithm, a is of the forms: $3q, 3q+1$ or $3q+2$.

If $a = 3q$, then

$$a(a+1)(a+2) = 3q(3q+1)(3q+2)$$
$$\Rightarrow 3|a(a+1)(a+2)$$

If $a = 3q+1$, then

$$a(a+1)(a+2) = (3q+1)(3q+1+1)(3q+1+2)$$
$$= (3q+1)(3q+2)(3q+3)$$
$$3(3q+1)(3q+2)(q+1)$$
$$\therefore \quad 3|a(a+1)(a+2)$$

If $a = 3q+2$, then

$$a(a+1)(a+2) = (3q+2)(3q+2+1)(3q+2+2)$$
$$= (3q+2)(3q+3)(3q+4)$$
$$= 3(3q+2)(q+1)(3q+4)$$
$$\therefore \quad 3|a(a+1)(a+2)$$

(b) Since a is any integer, so by division algorithm, a is of the forms: $3q, 3q+1, 3q+2$.

If $a = 3q$, then

$$a(2a^2+7) = 3q\{2(3q)^2+7\}$$
$$= 3q(18q+7)$$
$$\Rightarrow 3|a(2a^2+7)$$

If $a = 3q+1$, then

$$a(2a^2+7) = (3q+1)\{2(3q+1)^2+7\}$$
$$= (3q+1)\{2(9q^2+6q+1)+7\}$$
$$= (3q+1)(18q^2+12q+9)$$
$$= 3(3q+1)(6q^2+4q+3)$$
$$\Rightarrow 3|a(2a^2+7)$$

If $a = 3q+2$, then

$$a(2a^2+7) = (3q+2)\{2(3q+2)^2+7\}$$
$$= (3q+2)\{2(9q^2+12q+4)+7\}$$
$$= (3q+2)(18q^2+24q+15)$$
$$= 3(3q+2)(6q^2+8q+5)$$
$$\Rightarrow 3|a(3a^2+7)$$

Example 6: If $c = ax + by$ and $d|a$ but $d \nmid c$, then show that $d \nmid b$.

Solution: Let $c = ax + by$ and $d|a$ but $d \nmid c$.

Since $d|a$, therefore there exists q_1 such that $a = dq_1$.

Then $c = ax + by = dq_1x + by$.

If possible, let $d|b$. Then there exists an integer q_2 such that $b = dq_2$. Therefore

$$c = dq_1x + dq_2y$$
$$= d(q_1x + q_2y)$$
$$\Rightarrow d|c, \text{ which contradicts our assumption.}$$

Hence $d \nmid b$.

Example 7: If $a - s|ab + st$, then $a - s|at + bs$.

Solution: We have

$$(ab + st) - (at + bs) = (a - s)(b - t)$$

We have

$$a - s|ab + st \text{ and } a - s|(a - s)(b - t)$$
$$\Rightarrow a - s|at + bs$$

W CHECK YOUR PROGRESS

Q 1. For $n \geq 1$, use mathematical induction to establish each of the following divisibility statements:

(a) $21|4^{n+1} + 5^{2n-1}$

(b) $24|2.7^n + 3.5^n - 5$

Q 2. Prove that for any integer a, one of the integers $a, a + 2, a + 4$ is divisible by 3.

Q 3. If a is an arbitrary odd integer, then

$$32|(a^2 + 3)(a^2 + 7)$$

Q 4. Prove that if a and b are both odd integers, then $16|a^4 + b^4 - 2$.

2.5 TESTS OF DIVISIBILITY

Definition 2.5.1 Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n , symbolized by

$$a \equiv b(mod\ n)$$

If $n|a - b$, i.e.$a - b = kn$ for some integer k.

For example, (i) $7|24 - 3 \Rightarrow 24 \equiv 3(mod\ 7)$

(ii) $3|10-1 \Rightarrow 10 \equiv 1(mod\ 3)$

Properties of Congruences:

Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a(mod\ n)$

(b) If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$

(c) If $a \equiv b(mod\ n)$, $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$

(d) If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$, then $a + c \equiv b + d(mod\ n)$ and $ac \equiv bd(mod\ n)$

(e) If $a \equiv b(mod\ n)$, then $a + c \equiv b + c(mod\ n)$ and $ac \equiv bc(mod\ n)$

(f) If $a \equiv b(mod\ n)$, then $a^k \equiv b^k(mod\ n)$ for any positive integer k.

Theorem 2.5.2 Let N be a positive integer such that $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$, where $a_m \neq 0, 0 \leq a_i < 10$, for $0 \leq i \leq m-1$. Then

(a) $2|N \Leftrightarrow 2|a_0$

(b) $3|N \Leftrightarrow 3|\sum_{i=0}^{m} a_i$

(c) $4|N \Leftrightarrow 4|a_0 + 2a_1$

(d) $5|N \Leftrightarrow 5|a_0$

(e) $9|N \Leftrightarrow 9|\sum_{i=0}^{n} a_i$

(f) $11|N \Leftrightarrow 11|\sum_{i=0}^{m}(-1)^i a_i$

Proof: Since

$$10 \equiv \begin{cases} 0(mod\ 2)\ and\ \ 0(mod\ 5) \\ 1(mod\ 3)\ and\ \ 1(mod\ 9) \\ 2(mod\ 4) \\ -1(mod\ 11) \end{cases}$$

Therefore

$$N \equiv \begin{cases} a_0(mod\ 2)\ \ and\ \ a_0(mod\ 5) \\ \sum_{i=0}^{m} a_i\ (mod\ 3)\ and\ \ \sum_{i=0}^{m} a_i\ (mod\ 9) \\ 2a_1 + a_0(mod\ 4) \\ \sum_{i=0}^{m}(-1)^i a_i\ (mod\ 11) \end{cases}$$

Hence

$$2|N \Leftrightarrow 2|a_0 \quad \text{and} \quad 5|N \Leftrightarrow 5|a_0$$

$$3|N \Leftrightarrow 3|\sum_{i=0}^{m} a_i \ \text{ and } \ 9|N \Leftrightarrow 9|\sum_{i=0}^{m} a_i$$

$$4|N \Leftrightarrow 4|2a_1 + a_0$$

$$11|N \Leftrightarrow 11|\sum_{i=0}^{m}(-1)^i a_i.$$

Example 8: Show that 176521221 is divisible by 9.

Solution: Since $1+7+6+5+2+1+2+2+1=27$ and $9|27$, therefore $9|176521221$.

Example 9: Show that 502678 is divisible by 11.
Solution: Since $8-7+6-2+0-5=0$ and $11|0$, therefore $11|502678$.

Example 10: Show that 234284 is divisible by 4.
Solution: Here $a_1=8, a_0=4$.
Since $2a_1+a_0=2.8+4=20$ and $4|20$, therefore $4|234284$.

Theorem 2.5.3 (Divisibility Test for 7 or 13)
A number $N=a_{k-1}a_{k-2}\ldots.a_1a_0$ is divisible by 7 (or 13) if and only if $(a_2a_1a_0)-(a_5a_4a_3)+(a_8a_7a_6)-\cdots$ is divisible by 7 (or 13).

Proof: We have

$$N=a_{k-1}a_{k-2}\ldots a_2a_1a_0$$

It can be written as

$$N=(a_2a_1a_0)+(a_5a_4a_3)\times 1000+(a_8a_7a_6)\times 1000^2+\cdots$$

But $1000\equiv -1(mod\ 7)$ and $-1(mod\ 13)$
Therefore

$$N\equiv (a_2a_1a_0)+(a_5a_4a_3)\times(-1)+(a_8a_7a_6)\times(-1)^2+\cdots(mod\ 7\ or\ 13)$$
$$\Rightarrow N\equiv (a_2a_1a_0)-(a_5a_4a_3)+(a_8a_7a_6)-\cdots(mod\ 7)\ or\ \ (mod\ 13)$$

Hence

$$7|N\Leftrightarrow 7|(a_2a_1a_0)-(a_5a_4a_3)+(a_8a_7a_6)-\cdots$$

and

$$13|N\Leftrightarrow 13|(a_2a_1a_0)-(a_5a_4a_3)+(a_8a_7a_6)-\cdots$$

Example 11: Show that 2587322568103 is divisible by 7 and 13.
Solution: Here we have

$$N=2587322568103$$

and $103-568+322-587+2=-728$, which is divisible by 7 and 13. Therefore N is divisible by 7 and 13.

Another Method of Divisibility Test for 7(Doubling and Subtracting Method)
1. Take the last digit of the number.
2. Double that last digit.
3. Subtract the result from the rest of the number.
4. If the result is zero or a multiple of 7, then the original number is divisible by 7.
5. If the result is still a large number, repeat the process.

Example 12: Check if 33502 is divisible by 7.
Solution: Last digit= 2
Double it= 2
Remaining number= 3350

Subtract= $3350 - 4 = 3346$
which is a large number, so we apply the same process:
Last digit= 6
Double it= 12
Remaining number= 334
Subtract= $334 - 12 = 322$
Which is again a large number, so we again apply the same process:
Last digit= 2
Double it= 4
Subtract 4 from remaining number= $32 - 4 = 28$
Which is divisible by 7, so the original number 33502 is divisible by 7.

Divisibility Test for 6
A number divisible by 6 if and only if it is divisible by 2 and 3.

Example 13: Show that 2748 is divisible by 6.
Solution: Since $2|8$, so 2748 is divisible by 2. Also $2 + 7 + 4 + 8 = 21$ is divisible by 3, so 2748 is divisible by 3.

Since 2748 is divisible by 2 and 3, so it is divisible by 6.

Theorem 2.5.4 (Divisibility Test for 37)
A number $N = (a_{k-1}a_{k-2} \dots a_2a_1a_0)$ is divisible by 37 if $(a_2a_1a_0) + (a_5a_4a_3) + \cdots$ is divisible by 37.

Proof: Here $N = (a_{k-1}a_{k-2} \dots a_2a_1a_0)$, which can be written as $N = (a_2a_1a_0) + (a_5a_4a_3) \times 1000 + (a_8a_7a_6) \times 1000^2 + \cdots$

Since $1000 \equiv 1(mod\ 37)$, therefore

$$N = (a_2a_1a_0) + (a_5a_4a_3) + \cdots (mod\ 37)$$

Hence $37|N \Leftrightarrow 37|(a_2a_1a_0) + (a_5a_4a_3) + \cdots$

Example 14: Show that the number 22125744515 is divisible by 37.
Solution: Here $N = 22125744515$
and $515 + 744 + 125 + 22 = 1406$
which is divisible by 37. Therefore the given number is divisible by 37.

Theorem 2.5.5 (Divisible Test for 101)
A number $N = (a_{k-1}a_{k-2} \dots a_2a_1a_0)$ is divisible by 101 if and only if $101|(a_1a_0) - (a_3a_2) + (a_5a_4) - \cdots$

Proof: $N = (a_{k-1}a_{k-2} \dots a_2a_1a_0)$ can be written as

$$N = (a_1a_0) + (a_3a_2) \times 100 + (a_5a_4) \times 100^2 + \cdots$$

Since $100 \equiv -1(mod\ 101)$, therefore

$$N \equiv (a_1a_0) - (a_3a_2) + (a_5a_4) - \cdots (mod\ 101)$$

Hence $101|N \Leftrightarrow N|(a_1a_0) - (a_3a_2) + (a_5a_4) - \cdots$

Example 15: Show that the number 58533742 is divisible by 101.
Solution: Here $N = 58533742$ and $42 - 37 + 53 - 58 = 0$, which is divisible by 101.
Therefore the given number N is divisible by 101.

Theorem 2.5.6 (Divisibility Test for 2^h)
A number $N = (a_{k-1}a_{k-2} \dots a_2a_1a_0)$ is divisible by 2^h if and only if the number represented by the last h digits is divisible by 2^h, where h is a positive integer.

Proof: The number $N = (a_{k-1}a_{k-2} \dots a_2a_1a_0)$ can be written as $N = a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \cdots + a_h10^h + a_{h-1}10^{h-1} + \cdots + a_110 + a_0$.
Since 2^h divides 10^h and higher powers of 10, therefore $2^h|N \Leftrightarrow 2^h$ divides $a_{h-1}10^{h-1} + \cdots + 1_110 + a_0$.

Example 16: Show that 36536 is divisible by 8.
Solution: We have

$$N = 36536$$
$$= 3.10^4 + 6.10^3 + 5.10^2 + 3.10 + 6.1$$

Since $8 = 2^3|5.10^2 + 3.10 + 6 = 536$, therefore $8|36536$.

Example 17: Show that 4523936 is divisible by 32.
Solution: We have

$$N = 4523936$$
$$= 4.10^6 + 5.10^5 + 2.10^4 + 3.10^3 + 9.10^2 + 3.10 + 6$$

Since

$$32 = 2^5|2.10^4 + 3.10^3 + 9.10^2 + 3.10 + 6 = 23936$$

Therefore

$$32|4523936$$

W CHECK YOUR PROGRESS

Q 5. Find the missing digit of the number 95555_4353 so that it is divisible by 11.
Q 6. Show that 125671221 is divisible by 9.
Q 7. Test the number 67058902 for divisibility by 7.
Q 8. Let $N = a_m10^m + a_{m-1}10^{m-1} + \cdots + a_210^2 + a_110 + a_0$, where $0 \leq a_k \leq 9$ be the decimal expansion of a positive integer N. Prove that $6|N \Leftrightarrow 6|a_0 + 4a_1 + 4a_2 + \cdots + 4a_m$.
Q 9. Without performing the divisions, determine whether the integer 1010908899 is divisible by $7, 11$ and 13.
Q 10. Given an integer N, let M be the integer formed by reversing the order of the digits of N. Verify $N - M$ is divisible by 9.

22.6 LET US SUM UP

- **Divisibility:** An integer b is said to be divisible by an integer $a \neq 0$, in symbols $a|b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.
- For integers a, b, c the following hold:
  (a) $a|0, 1|a, a|a$
  (b) $a|1 \Leftrightarrow a = \pm 1$
  (c) $a|b, c|d \Rightarrow ac|bd$
  (d) $a|b, b|c \Rightarrow a|c$
  (e) $a|b, b|c \Leftrightarrow a = \pm b$
  (f) $a|b, b \neq 0 \Rightarrow |a| \leq |b|$
  (g) $a|b, a|c \Rightarrow a|bx + cy$ for arbitrary integer
- Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b(mod\ n)$ if $n|a - b$.
- Let N be a positive integer such that

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$$

Where $a_m \neq 0$ and $0 \leq a_i < 10$ for $0 \leq i \leq m - 1$.

Then (i) $2|N \Leftrightarrow 2|a_0$
(ii) $3|N \Leftrightarrow 3|\sum_{i=0}^{m} a_i$
(iii) $4|N \Leftrightarrow 4|2a_1 + a_0$
(iv) $5|N \Leftrightarrow 5|a_0$
(v) $9|N \Leftrightarrow 9|\sum_{i=0}^{m} a_i$
(vi) $11|N \Leftrightarrow 11|\sum_{i=0}^{m} (-1)^i a_i$

- **Divisibility Test for 7 or 13:** A number $N = (a_{k-1}a_{k-2} \ldots a_2 a_1 a_0)$ is divisible by 7 or 13 if and only if $(a_2 a_1 a_0) - (a_5 a_4 a_3) + (a_8 a_7 a_6) - \cdots$ is divisible by 7 or 13.
- **Divisibility Test for 37:** A number $N = (a_{k-1}a_{k-2} \ldots a_2 a_1 a_0)$ is divisible by 37 if and only if $37|(a_2 a_1 a_0) + (a_5 a_4 a_3) + \cdots$
- **Divisibility Test for 101:** A number $N = (a_{k-1}a_{k-2} \ldots a_2 a_1 a_0)$ is divisible by 101 if and only if $101|(a_1 a_0) - (a_3 a_2) + (a_5 a_4) - \cdots$
- **Divisibility Test for 2^h, h is a positive integer:** A number $N = (a_{k-1}a_{k-2} \ldots a_2 a_1 a_0)$ is divisible by 2^h if and only if the number represented by the last h digits is divisible by 2^h.

K 2.7 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q 1. (a) Let

$$P(n): 21|4^{n+1} + 5^{2n-1}$$

For $n = 1$, $4^{1+1} + 5^{2.1-1} = 21$, which is divisible by 21.
Therefore $P(1)$ is true.
We assume $P(k)$ is true for any positive integer k, i.e.

$$21|4^{k+1} + 5^{2k-1}$$

$$\Rightarrow 4^{k+1} + 5^{2k-1} = 21x \text{ for some integer } x$$

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

$$4^{(k+1)+1} + 5^{2(k+1)-1} = 4.4^{k+1} + 5^{2k+1}$$

$$= 4.4^{k+1} + 5^2.5^{2k-1} + 4.5^{2k-1} - 4.5^{2k-1}$$

$$= 4\left(4^{k+1} + 5^{2k-1}\right) + 21.5^{2k-1}$$

$$= 4.21x + 21.5^{2k-1}$$

$$21\left(4x + 5^{2k-1}\right)$$

$$\therefore \ 21|4^{(k+1)+1} + 5^{2(k+1)-1}$$

Therefore $P(k+1)$ is true. Hence by mathematical induction, $P(n)$ is true for all integers $n \geq 1$, i.e.,

$$21|4^{n+1} + 5^{2n-1} \text{ for all integers } n \geq 1.$$

(b) Let the given statement be $P(n)$, i.e.

$$P(n): 24|2.7^n + 3.5^n - 5$$

For $n = 1$, $2.7^1 + 3.5^1 - 5 = 24$, which is divisible by 24.
Therefore $P(1)$ is true.
We assume $P(k)$ is true for any integer k, i.e.

$$24|2.7^k + 3.5^k - 5$$

$$\Rightarrow 2.7^k + 3.5^k - 5 = 24x \text{ for some integer } x \qquad (1)$$

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

$$2.7^{k+1} + 3.5^{k+1} - 5 = 7.\left(2.7^k\right) + 5\left(3.5^k\right) - 5$$

$$= 2.\left(2.7^k\right) + 5\left(2.7^k\right) + 5\left(3.5^k\right) - 5 + 5.5 - 5.5$$

$$= 5\left(2.7^k + 3.5^k - 5\right) + 2.\left(2.7^k\right) - 5 + 5.5$$

$$= 5.24x + 4.7^k + 20 \qquad \text{[using (1)]} \qquad (2)$$

Let $q(k) \equiv 24|4.7^k + 20$
For $k = 1$, $4.7^1 + 20 = 48$, which is divisible by 24.
Therefore $q(1)$ is true.
Suppose $q(s)$ is true for some positive integer s. i.e.

$$24|4.7^s + 20$$

$$\Rightarrow 4.7^s + 20 = 24y \text{ for some integer } y$$

$$\Rightarrow 4.7^s = 24y - 20 \qquad (3)$$

Now we prove $q(s+1)$ is true.

$$4.7^{s+1} + 20 = 4.7^s.7 + 20$$

$$= (24y - 20)7 + 20 \quad \text{[using (3)]}$$
$$= 7.24y - 120$$
$$= 24(7y - 5)$$
$$\therefore \ 24|4.7^{s+1} + 20$$

Therefore $q(s+1)$ is true. By principle of mathematical induction $q(k)$ is true for any positive integer k, i.e.

$$24|4.7^k + 20$$
$$\Rightarrow 4.7^k + 20 = 24z \text{ for some integer } z$$

From (2), $2.7^{k+1} + 3.5^{k+1} - 5 = 5.24x + 24z$
$$= 24(5x + z)$$
$$\Rightarrow 24|2.7^{k+1} + 3.5^{k+1} - 5$$

Hence $P(k+1)$ is true. By principle of mathematical induction, $P(n)$ is true for all $n \geq 1$, i.e.

$$24|2.7^n + 3.5^n - 5 \text{ for all integer } n \geq 1.$$

Answer to Q 2. By division algorithm, any integer is of the form $3q, 3q+1, 3q+2$.
Suppose $3 \nmid a$. Then a is of the forms: $3q+1$ or $3q+2$.
If $a = 3q+1$, then $a + 2 = (3q+1) + 2 = 3q + 3 = 3(q+1)$
$$\Rightarrow 3|a+2$$
If $a = 3q+2$, then $a + 4 = (3q+2) + 4 = 3q + 6 = 3(q+2)$
$$\Rightarrow 3|a+4$$
Thus if $3 \nmid a$, then either $3|a+2$ or $3|a+4$.
Suppose $3 \nmid a+2$. Then $a+2$ is of the forms: $3q+1$ or $3q+2$.
If $a+2 = 3q+1$, then $a+4 = (a+2)+2 = (3q+1)+2 = 3(q+1)$
$$\Rightarrow 3|a+4$$
If $a+2 = 3q+2 \Rightarrow a = 3q \Rightarrow 3|a$
Thus, if $3 \nmid a+2$, then $3|a$ or $3|a+4$.
Suppose $3 \nmid a+4$. Then $a+4$ is of the forms: $3q+1$ or $3q+2$.
If $a+4 = 3q+1$, then $a+2 = (a+4)-2$
$$= (3q+2) - 2$$
$$= 3q$$
$$3|a+2$$
Thus, if $3 \nmid a+4$, then $3|a$ or $3|a+2$.
Hence for integer a, one of $a, a+2, a+4$ is divisible by 3.

Answer to Q 3. Since a is odd, therefore a is of the form $2q+1$, where $q \in Z$. Then

$$(a^2+3)(a^2+7) = \{(2q+1)^2 + 3\}\{(2q+1)^2 + 7\}$$

$$= (4q^2 + 4q + 4)(4q^2 + 4q + 8)$$

$$= 16q^4 + 32q^3 + 64q^2 + 48q + 32$$

If q is even, i.e., $q = 2n$, then

$$(a^2+3)(a^2+7) = 16.(2n)^4 + 32(2n)^3 + 64(2n)^2 + 48.2n + 32$$

$$= 32(8n^4 + 8n^3 + 8n^2 + 3n + 1)$$

$$\Rightarrow 32|(a^2+3)(a^2+7)$$

If q is odd, i.e. $q = 2n+1$, then

$$(a^2+3)(a^2+7) = 16(2n+1)^4 + 32(2n+1)^3 + 64(2n+1)^2 + 48(2n+1) + 32$$

$$= 256n^4 + 64.8n^3 + 384n^2 + 128n + 16 + 32.8n^3 + 96.4n^2 + 192n + 32 + 256n^2 + 256n + 64 + 96n + 48 + 32$$

$$= 256n^4 + 768n^3 + 1024n^2 + 672n + 192$$

$$= 32(8n^4 + 24n^3 + 32n^2 + 21 + 6)$$

Therefore $32|(a^2+3)(a^2+7)$.

Answer to Q 4. Let $a = 2r+1, b = 2s+1$.

Then

$$a^4 + b^4 - 2 = (2r+1)^4 + (2s+1)^4 - 2$$

$$= 16(r^4 + s^4) + 32(r^3 + s^3) + 24(r^2 + s^2) + 8(r+s) \qquad (*)$$

All terms are divisible by 16 except $24r^2 + 8r$ and $24s^2 + 8s$.

If r is even, i.e. $r = 2n$ for some integer n, then

$$24r^2 + 8r = 24.(2n)^2 + 8.2n$$

$$= 16(6n^2 + n)$$

$$\Rightarrow 16|24r^2 + 8r$$

If r is odd, i.e. $r = 2n+1$, for some $n \in Z$, then

$$24r^2 + 8r = 24(2n+1)^2 + 8(2n+1)$$

$$= 24(4n^2 + 4n + 1) + 16n + 8$$

$$= 96n^2 + 96n + 24 + 16n + 8$$

$$= 96n^2 + 112n + 32$$

$$= 16(6n^2 + 7n + 2)$$

$\therefore \quad 16|24r^2 + 8r \Rightarrow 24r^2 + 8r = 16p$, for some integer p

Similarly we can show that

$16|24s^2 + 8s \Rightarrow 24s^2 + 8s = 16q$, for some integer q

From $(*)$, we obtain

$$a^4 + b^4 - 2 = 16(r^4 + s^4) + 32(r^3 + s^3) + 16p + 16q$$

$$= 16\{(r^4 + s^4) + 2(r^3 + s^3) + p + q\}$$

$$\Rightarrow 16|a^4 + b^4 - 2$$

Answer to Q 5. Here $N = 95555_4353$

Suppose the missing digit is x. Since N is divisible by 11, therefore

$$11|3 - 5 + 3 - 4 + x - 5 + 5 - 5 + 5 - 9$$

$$\Rightarrow 11|x - 12$$

$$\Rightarrow x = 1 \text{ as } 0 \leq x < 10$$

Hence the missing digit is 1.

Answer to Q 6. Left as an exercise.

Answer to Q 7. Left as an exercise.

Answer to Q 8. We have

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0, \quad 0 \leq a_k \leq 9$$

We have

$10 \equiv 4(mod\ 6)$ and $40 \equiv 4(mod\ 6)$

We have to prove $P(n): 10^n \equiv 4(mod\ 6)$ is true for all $n \geq 1$.

For $n = 1, 10 \equiv 4(mod\ 6)$, i.e. $P(1)$ is true.

Suppose $P(k)$ is true, i.e. $10^k \equiv 4(mod\ 6)$

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

Now

$$10^{k+1} = 10^k.10 \equiv 4.10(mod\ 6)$$

$$\Rightarrow 10^{k+1} \equiv 40(mod\ 6)$$

$$\Rightarrow 10^{k+1} \equiv 4(mod\ 6) \quad [since\ 40 \equiv 4(mod\ 6)]$$

Hence by the principle of mathematical induction, $P(n)$ is true for all integer $n \geq 1$, i.e.

$$10^n \equiv 4(mod\ 6) \text{ for } n \geq 1$$

$$N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

$$\equiv 4a_m + 4a_{m-1} + \cdots + 4a_2 + 4a_1 + a_0(mod\ 6)$$

$$\Rightarrow 6|N \Leftrightarrow 6|a_0 + 4a_1 + 4a_2 + \cdots + 4a_{m-1} + 4a_m$$

Answer to Q 9. Left as an exercise.

Answer to Q 10. Let

$$N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$$

$$M = a_0 10^m + a_1 10^{m-1} + \cdots + a_{m-1}10 + a_m$$

Therefore

$$N - M = (a_m - a_0)10^m + (a_{m-1} - a_1)10^{m-1} + \cdots (a_1 - a_{m-1})10 + (a_0 - a_m)$$

The sum of the coefficients of $N - M$ is

$$(a_m - a_0) + (a_{m-1} - a_1) + \cdots + (a_1 - a_{m-1}) + (a_0 - a_m)$$

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

$$= 0$$

Since $9|0$, therefore $9|N-M$.

O 2.8 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 2.9 MODEL QUESTIONS

1. Establish the followings:
   (a) If a is an arbitrary integer, then $6|a(a^2+11)$.
   (b) If a is an odd integer, then $24|a(a^2-1)$.
   (c) If a and b are odd integers, then $8|a^2-b^2$.
2. Without performing the divisions, determine whether the integers 176521221 and 149235678 are divisible by 9 or 11.
3. Let $R_n = 111\ldots11$ (for example, $R_5 = 11111$). Show that
   (a) $9|R_n$ if and only if $9|n$.
   (b) $11|R_n$ if and only if n is even.
4. If 495 divides $273x49y5$, then obtain the digits x and y.
5. If 792 divides the integer $13xy45z$, then find the digits x, y and z.

*** *** ***