MANGALAYATAN UNIVERSITY
Learn Today to Lead Tomorrow
NAAC GRADE A+ Accredited University

BACHELOR OF COMPUTER APPLICATIONS (BCA)

CSB-1113 (Mathematics - I)

Block 1: Introduction to Sets Functions and Numbers

Unit 3: Division Algorithm, Greatest Common Divisor, The Euclidean Algorithm

Structure

3.1 INTRODUCTION

In elementary number theory, several fundamental concepts and algorithms play a crucial role in understanding and manipulating integers. Among these are the Division Algorithm, Greatest Common Divisor (GCD), and the Euclidean Algorithm. These concepts provide essential tools for solving problems related to divisibility, factorization, and solving linear Diophantine equations.

The Division Algorithm serves as the foundation for understanding the properties of division in the realm of integers. It provides a systematic method for dividing one integer by another, yielding both a quotient and a remainder. By expressing any integer a as the product of another integer b and a quotient q, plus a remainder r, the Division Algorithm formalizes the process of integer division.

The Greatest Common Divisor (GCD) is a fundamental concept in number theory, representing the largest integer that divides two given integers without leaving a remainder. Understanding the GCD is essential for simplifying fractions, finding common factors, and solving various mathematical problems, such as finding the least common denominator or reducing fractions to lowest terms.

The Euclidean Algorithm is an efficient and ancient method for computing the GCD of two integers. It relies on the principle that the GCD of two integers remains unchanged when one integer is replaced by its remainder upon division by the other. By iteratively applying this process, the Euclidean Algorithm efficiently computes the GCD, providing a reliable method for finding the greatest common divisor of any two integers.

Together, these concepts and algorithms form the cornerstone of elementary number theory, enabling mathematicians and students to explore the properties and relationships of integers in a systematic and rigorous manner. Whether used for solving practical problems or exploring theoretical concepts, the

Division Algorithm, Greatest Common Divisor, and the Euclidean Algorithm are indispensable tools in the study of number theory and its applications.

3.2 OBJECTIVES

After going through this unit, students will be able to

- Understand the concept of Division Algorithm
- Define Greatest Common Divisor
- Apply Euclidean Algorithm to calculate the GCD of two integers

3.3 DIVISION ALGORITHM

From elementary mathematics we know that

- Sum of two integers is an integer.
- Difference of two integers is an integer.
- Product of two integers is an integer.

Therefore, In the language of modern algebra we can say that, the set of all integers $\mathbb{Z}$ is closed with respect to operation of addition, subtraction and multiplication. However, when we consider the operation of division of one integer by another integer, we see that the result is not always an integer.

Multiple: Let a be any integer and k be an arbitrary integer. Then the number am is called a multiple of a.

Note: 1. 0 is multiple of every integer.

2. There are infinitely many multiples of any non-zero integer.

Divisibility: An integer a is said to be divisible by a non-zero integer b if $a = bq$ for some integer q. In alternative forms, we can also write this fact as

- b is a divisor of a.
- b divides a.
- $b \mid a$ or $b|a$.
- a is a multiple of b.

Division Algorithm:

Theorem 1: For given integers a and $b > 0$. Then there exist unique integers q and r called respectively quotient and remainder such that $a = bq + r, 0 \leq r < b$

Proof: Consider the infinite sequence of multiples of b:

$$\ldots, -b, 0, b, \ldots, bq, \ldots$$

Obviously a must be equal to one of the multiples of b say bq in the sequence, or must be between two consecutive multiples say bq and $b(q+1)$.

In either case we have $bq \leq a < b(q+1)$ for some q. This iniplies $0 \leq a - bq < b$. Let us put $a - bq = r$. Then we have $a = bq + (a - bq) = bq + r, 0 \leq r < b$. This proves the main part of the theorem, namely the existence of q and r.

We still have to prove that the integers q and r are unique. Suppose they are not unique. Then it follows that

$$a = bq + r, \quad 0 \leq r < b$$
$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

for some integers q, r, q_1 and r_1. These two equations imply $r_1 - r = b(q - q_1)$. Hence b divides $r_1 - r$. But this is impossible since both r and r_1 are positive and less than b, therefore q and r are unique.

In the above proof we notice that $bq \leq a < b(q + 1)$. Hence, we have the following result,

Result: bq is the largest multiple of b which does not exceed a.
In the Division Algorithm r is called the least non-negative remainder of a with respect to b, or briefly the remainder of a with respect to b. q is called the quotient of a with respect to b.

Minimal remainder: In the division algorithm explained earlier the remainder is always positive and less than b. However, it is possible to have another kind of division algorithm in which the remainder does not numerically exceed $\frac{b}{2}$. For example, let $a = 37$ and $b = 8$. Then by division algorithm we have

$$37 = 8 \times 4 + 5, \qquad 0 < 5 < 8. \tag{1}$$

Here 5 is the (least non-negative) remainder. But (1) can be put in another form as below:

$$37 = 8 \times 5 + (-3), \tag{2}$$

where $0 < |-3| < \frac{8}{2}$. Here -3 is numerically less than half the divisor 8. We call such a remainder by the name minimal remainder or the absolutely least remainder. As another exayple we take $a = 71$ and $b = 17$ then we have $71 = 17 \times 4 + 3$. Here $0 < 3 < 17$ and also $0 < |3| < \frac{17}{2}$. Therefore 3 is the remainder as well as minimal remainder. The division algorithm theorem for minimal remainder is as follows:

Theorem 2: Let a and b be any two integers, $b > 0$. Then there erist integers Q and R such that $a = bQ + eR, 0 < R < \frac{b}{2}$, where $e = +1$ or -1.

Proof: By Theorem 1 we have

$$a = bq + r, 0 \leq r < b.$$

Case 1: Let $r < \frac{b}{2}$. If we let $Q = q, R = r$ and $e = 1$, then (1) is changed to $a = bQ + eR, 0 \leq R < \frac{b}{2}$.
Case 2: Let $r > \frac{b}{2}$, so that we have $0 < b - r < \frac{b}{2}$. If we let $Q = q + 1, R = b - r$ and $\dot{e} = -1$ then (1) is transformed to $a = b(q + 1) - (b - r) = bQ + eR, 0 \leq R < \frac{b}{2}$.
Case 3: Let $r = \frac{b}{2}$. In this case if we put $Q = q, R = r$ and $e = 1$ in (1) then we obtain $a = bQ + eR, R = b/2$. Alternatively, if we put in (1) $Q = q + 1, R = b - r$ and $e = -1$ we obtain $a = b(q + 1) - (b - r) = bQ + cR, R = \frac{b}{2}$. This completes the proof of the Theorem.

The following remark should be particularly noted

Remark: 1. In the above theorem, since q and r are unique, it follows that Q and R are also unique except when $R = \frac{b}{2}$

2. R is called the minimal remainder (or the absolutely least remainder) of a with respect to b. Observe that

(i) If $r < \frac{b}{2}$, then the minimal remainder is r.

(ii) If $r > \frac{b}{2}$, then the minimal remainder is $-(b-r)$.

(iii) If $r = \frac{b}{2}$, then the minimal remainder may be taken as r or $-r$ according to our choice.

Example 1: Find the minimal remainder of 217 with respect to 39.

Solution: Because $217 = 39 \times 5 + 22$

By comparing with $a = bq + r$, we have

$$a = 217, b = 39, q = 5, r = 22$$
$$22 > \frac{39}{2} \text{ i.e., } r > b/2$$

Here

$$22 > \frac{39}{2} \text{ i.e., } r > b/2$$

Then minimal remainder $= -(b-r)$

$$= -(39-22) = -17$$

Example 2: Find the minimal remainder of 171 with respect to 23.

Solution: Because $171 = 23 \times 7 + 10$

Here

$$10 < \frac{23}{2} \text{ i.e., } r < b \mid 2$$

Then minimal remainder = r = 10

Theorem 3: Every integer is of the form

(i) $3q$ or $(3q \pm 1)$
(ii) $4q, (4q \pm 1)$ or $(4q \pm 2)$
(iii) $5q, (5q \pm 1)$ or $(5q \pm 2)$

Proof: Because for any two integers a and $b > 0$ there exist integers q_1 and r_1 such that

$$a = bq_1 + er_1, \qquad 0 \le r_1 < \frac{b}{2}, \qquad \text{e} = 1 \text{ or } -1 \qquad (1)$$

(i) To take $b = 3$ in $eq^n(1)$, we get

$$a = 3q_1 + er_1, \qquad 0 \le r_1 < \frac{3}{2}, \qquad e = \pm 1$$

Therefore $r_1 = 0$ or 1. Hence $a = 3q$ or $a = 3q \pm 1$

(ii) To take $b = 4$ in $eq^n(1)$, we get

$$a = 4q_1 + er_1, \qquad 0 \le r_1 < \frac{3}{2}, \qquad e = \pm 1$$

Therefore $r_1 = 0,1$ or 2. Hence $a = 4q, (4q \pm 1)$ or $4q \pm 2$.

(iii) To take $b = 5$ in $eq^n(1)$, we get

$$a = 5q_1 + er_1, \qquad 0 \le r_1 < \frac{5}{2}, \qquad e = \pm 1$$

Therefore $r_1 = 0,1$ or 2. Hence $a = 5q, (5q \pm 1)$ or $5q \pm 2$.

Example 3: One of every three consecutive Integers is divisible by 3.

Solution: Let $n, (n+1), (n+2)$ be any three consecutive integers.

Then n must be of the form $3q, (3q+1)$ or $(3q-1)$.

If $n = 3q \Rightarrow n$ is divisible by 3.

If $n = 3q+1$ then $n+2 = 3q+3 = 3(q+1)$

$\Rightarrow \quad (n+2)$ is divisible by 3.

If $n = 3q-1$ then $n+1 = 3q$

$\Rightarrow (n+1)$ is divisible by 3.

Hence one of every three consecutive integers is divisible by 3.

Example 4: The product of any three consecutive integers is divisible by 6 or 3!.

Solution: Let $a_1(a+1), (a+2)$ be any three consecutive integers then we have to show $a(a+1)(a+2)$ is divisible by $6 = 3!$ We will prove this result by mathematical induction.

Step I: Let

$$f(a) = a(a+1)(a+2) \tag{1}$$

Step II: To put $a = 1, f(1) = 1.\ (2)\ (3) = 6$

$\Rightarrow \quad f(a)$ is divisible by 6 for $a = 1$

Step III: Let $f(a)$ is divisible by 6 for some a.

$$\Rightarrow \quad a(a+1)(a+2) = 6k$$

Step IV: Now

$$\begin{aligned} f(a+1) \quad &= (a+1)(a+1+1)(a+1+2) \\ &= (a+1)(a+2)(a+3) \\ &= a(a+1)(a+2) + 3(a+1)(a+2) \end{aligned} \tag{2}$$

Because first term on of R.H.S. of eq(2) is divisible by $6 = 3!$ by our assumption. The second term is also divisible by 3! because $(a+1)(a+2)$ is divisible by $2! = 2$

$\Rightarrow$ R.H.S. of $\text{eq}^n(2)$ is divisible by $3! = 6$

$\Rightarrow f(a+1)$ will be divisible by 6.

Hence by mathematical induction the product of any three consecutive integers is divisible by 6.

Example 5: Prove that $9^n - 8^n - 1$ is divisible by 8.

Solution:

Step 1. Let $f(n) = 9^n - 8^n - 1$

Step II. To put $n = 1, f(1) = 9^1 - 8^1 - 1 = 0$

which is divisible by 8.

Step III. Let $f(n)$ is divisible by 8 for somen.

$$f(n) = 9^n - 8^n - 1 = 8k$$

Step IV. Now $f(n+1) = 9^{n+1} - 8^{n+1} - 1 = 9^n \cdot 9 - 8^n \cdot 8 - 1$

$$\begin{aligned} &= 9(9^n - 8^n - 1) + 8^n + 8 \\ &= 9 \cdot (8k) + 8^n + 8 \\ &= 8 \cdot [9k + 8^{n-1} + 1] \end{aligned}$$

[By equation (2)]
$\Rightarrow f(n+1)$ is also divisible by 8,
Hence by mathematical induction $f(n)$ is divisible by 8.

Example 6: Prove that $2^{2n+1} - 9n^2 + 3n - 2$ is divisible by 54.

Solution:

Step I. Let $f(n) = 2^{2n+1} - 9n^2 + 3n - 2$

Step II. For $n = 1, f(1) = 2^{2\times1+1} - 9(1)^2 + 3(1) - 2 = 0$,

which is divisible by 54.

$\therefore$ The reault is true for $n = 1$

Step III. Let $f(n) = 2^{2n+1} - 9n^2 + 3n - 2$ be divisible by 54 for some n.

Then

$$f(n) = 2^{2n+1} - 9n^2 + 3n - 2 = 54k \qquad (1)$$

Step IV. Now $f(n+1) = 2^{2(n+1)+1} - 9(n+1)^2 + 3(n+1) - 2$

$$\begin{aligned}
&= 2^{2n+3} - 9(n^2 + 1 + 2n) + 3(n+1) - 2 \\
&= 2^2 \cdot 2^{2n+1} - 9n^2 - 15n - 8 \\
&= 4(2^{2n+1}) - 9n^2 - 15n - 8 \\
&= 4[2^{3n+1} - 9n^2 + 3n - 2] + 36n^2 - 12n + 8 - 9n^2 - 15n - 8 \\
&= 4[2^{2n+1} - 9n^2 + 3n - 2] + 27n^2 - 27n \\
&= 4(54k) + 27n(n-1)[\text{ By using eq } {}^{n}(1)] \\
&= 216k + 27.2t
\end{aligned}$$

$\because (n-1)n$ being is the product of 2 consecutive integers in divisible by 2! i.$e, 2$ hence $n(n-1) = 2t$]

$$= 216k + 54t = 54[4k + t]$$

or

$$\begin{aligned}
&= 216k + 54t = 54[4k + t] \\
f(n+1) \quad &= 54[4k + t]
\end{aligned}$$

$\Rightarrow \quad f(n+1)$ is divisible by 54.

Hence by mathematical induction $f(n)$ is divisible by 54.

3.4 GREATEST COMMON DIVISOR

Common Divisor: If a number c divides any two numbers a and b then c is known as a common divisor of a and b.

Greatest Common Divisor: The greatest common divisor (gcd) of numbers a and b is the unique positive integer " d " with the following two properties:

(i) $d|a$ and $d \mid b$
(ii) If $c \mid a$ and $c \mid b$, then $c \mid d$

Note: 1. The greatest common divisor is written as gcd in short.

Note: 2 The gcd of a and b is also written as $(a,\ b)$.

Note: 3 The gcd of $a_1, a_2, \ldots, a_k$ is written as $(a_1, a_2, \ldots, a_k)$.

For example:

1. $\gcd(12,18) = 6$
2. $\gcd(-5,5) = 5$
3. $\gcd(-8,-36) = 4$
4. $\gcd(8,15) = 1$

Remember Points :

(i) $(a,b) = (b,a)$
(ii) If $a \mid b$ then $(a,b) = a$

Theorem 1: The greatest common divisor is unique.

Proof: Let $a_1, a_2, \dots, a_k$ be the given integers and let d_1 and d_2 be their two $gcd's$. Then clearly d_1 divides $a_1, a_2, \dots, a_k$ and d_2 is their gcd. Then by the definition of gcd

(i) d_1 divides d_2. (ii) conversely it can be proved in a similar manner that d_2 divides d_1. Here (i) and (ii) imply that $d_1 = d_2$. This proves the theorem.

Theorem 2: Let $a_1, a_2, \dots, a_n$ be any non-zero integers whose gcd is d. Then there exist integers $x_1, x_2, \dots, x_n$ such that $a_1x_1 + a_2x_2 + \dots a_nx_n = d$.

Corollary: Let $(a,b) = d$. Then there exist integers x and y such that

$$ax + by = d.$$

Theorem 3: (Euclid's First Theorem) If c divides ab, $\gcd(a,c) = 1$ then c divides b.

Proof: Given that $\gcd(a,c) = 1$, then by the previous corollary there exist integers x and y such that $ax + cy = 1$. Multiplying this equation by b we get

$$abx + bcy = b \qquad (1)$$

Now c divides ab. Therefore c divides abx. Also c divides bcy. Then from (1) c divides b.

Example 1: Find gcd of 12 & 15.

Solution: Because $12 = 1 \times 2 \times 2 \times 3$ and $15 = 1 \times 3 \times 5$

Here $3 \mid 12$ and $3/15 \Rightarrow d = 3$

3.5 THE EUCLID's ALGORITHM

Euclid's Algorithm

The gcd of two integers " " and " b " can be determined by a process, which is known as Euclid's algorithm.

And more importantly Euclid's algorithm is a repeated application of division algorithm.

Euclid's algorithm is as follows:
Let a and b both are positive and $a > b$.
Then there exists q_1 and r_1 such that

$$a = bq_1 + n_1, \quad 0 \le n_1 < b \qquad (1)$$

(By using division algorithm)

Again there exists integers q_2 and r_2 such that

$$b = n_1q_2 + r_2, 0 \le r_2 < r_1 \qquad (2)$$

Now continuing this process, we have

$$r_1 = r_2 q_3 + r_3, \qquad 0 \le r_3 < r_2 \tag{3}$$

$$\vdots \quad \vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, \qquad r_n = 0 \tag{n}$$

Where $q_n \geq 2$

Here, we get $a > b > r_1 > r_2 > \cdots$ .....

Thus, these numbers form a decreasing sequence of non-negative numbers.

After a finite number of steps we will get $r_n = 0$ for some integer n and the process ends here.

The sets of equations (1) to (n) is called Euclid's algorithm for a and b.

Example: Determine $gcd(56,72)$.

Solution: If we divide 72 by 56, we get

$$72 = 56 + 16$$

Again divide 56 by 16 we get

$$56 = 16 \times 3 + 8$$

Again divide 16 by 8 we get

$$16 = 8 \times 2 + 0$$

Since the last non-zero remainder is 8, $gcd(56,72) = 8$.

$$\text{Also, } 8 = 56 - 16 \times 3 = 56 - (72 - 56) \times 3 = 56 \times (4) + 72 \times (-3)$$

Therefore $8 = 56x + 72y$, where $x = 4, y = -3$.

Which gives a way to find x, y such that $\gcd(a, b) = ax + by$.

3.6 LET US SUM UP

So, in this first unit we have learned about the following concepts

a) Division Algorithm

b) Greatest Common Divisor

c) Euclidean Algorithm

3.7 UNIT END EXERCISE

3.7.1 By using Euclid's algorithm show that

(i) Every odd integer is of the form $4k + 1$ or $4k + 3$.

(ii) The square of any integer is either of the form $3k$ or $3k + 1$.

(iii) The cube of any integer is of the form $9k, 9k + 1$or $3k + 1$.

3.7.2 Let $d = \gcd(826,\ 1890)$. Use Euclid's algorithm to compute d then find x, y such that $d = 826x + 1890y$.

3.7.3 If $\gcd(a, b) = 1$, show that $\gcd(a + b,\ a - b)$ is either 1 or 2.

3.8 REFERENCES AND SUGGESTED READINGS

I. David Burton, M. (2007). ELEMENTARY NUMBER THEORY Seventh Edition.

II. Rosen, K. H. (2011). *Elementary number theory*. London: Pearson Education.

III. Hari Kishan. (2014). Number Theory. Krishna Prakashan, Meerut.

***