UNIT 1: BASIC CONCEPTS

UNIT STRUCTURE

1.1 Learning Objectives
1.2 Introduction
1.3 Division Algorithm
1.4 Greatest Common Divisor (GCD)
1.5 Euclidean Algorithm
1.6 Least Common Multiple (LCM)
1.7 Kronecker's Theorem
1.8 Let Us Sum Up
1.9 Answers to Check Your Progress
1.10 Further Reading
1.11 Model Questions

1.1 LEARNING OBJECTIVES

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

- understand the statement of the division algorithm and its significance in number theory
- apply the division algorithm to express a given integer as a quotient and remainder
- define the greatest common divisor of two or more numbers
- find the GCD of two numbers using prime factorization
- apply properties of GCD
- understand the statement of Euclidean algorithm
- use the Euclidean algorithm to find the GCD of two integers
- define least common multiple and understand its significance
- compute the LCM and apply properties of LCM
- understand the statement of Kronecker's theorem
- apply the Kronecker's theorem in number theory

1.2 INTRODUCTION

Number theory is a branch of mathematics that studies the properties and relationships of numbers, particularly integers. It has applications in cryptography, computer science and pure mathematics. Below are some fundamental concepts in number theory.

1. **Divisibility and factor:** An integer a is divisible by another integer b if there exists an integer c such that $a = bc$.

2. **Prime numbers and composite numbers:** A prime number is a number greater than 1 that has exactly two divisors 1 and the number itself $(e.g. 2, 3, 5, 7, 11, \ldots.)$.

A composite number has more than two divisors $(e.g. 4, 6, 8, 9, 10, \ldots.)$.

3. **Division algorithm:** The division algorithm states that for any two integers a (dividend) and b (divisor, $b \neq 0$), there exist unique integers q (quotient) and r (remainder) such that

$$a = bq + r, \text{ where } 0 \leq r < |b|.$$

4. **Greatest Common Divisor (GCD) and Least Common Multiple (LCM):** The GCD of two numbers is the largest integer that divides both the numbers. e.g. $\gcd(12, 18) = 6$.

The LCM of two numbers is the smallest integer that is a multiple of both numbers. Example, $lcm(12, 18) = 36$.

5. **Euclidean Algorithm:** A method to compute the gcd of two numbers using repeated division. Example, $\gcd(48, 18) = 6$.

1.3 DIVISION ALGORITHM

Theorem 1.3.1 (Division Algorithm)

Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying $a = bq + r$, $0 \leq r < b$. The integers q and r are called respectively, the quotient and remainder in the division of a and b.

Proof: Let $S = \{a - bq | \ q \text{ is an integer}, a - bq \geq 0\}$.

Then $S \neq \phi$, as we take $q = -|a|$.

When $a > 0$, then $a - bq = a + b > 0$ as $b > 0$

$$\Rightarrow a - bq \in S$$

When $a < 0$, then $a - bq = a - ab = a(1 - b) \geq 0$

$$\Rightarrow a - bq \in S.$$

When $a = 0$, then $a - bq = 0 \Rightarrow a - bq \in S$.

By well ordering principle, S has a least element, say $r \in S$. Then $r = a - bq$ for some $q \in Z \Rightarrow a = bq + r, r \geq 0$.

Now we have to prove $r < b$. If possible, suppose

$$r \geq b$$
$$\Rightarrow a - bq \geq b$$
$$\Rightarrow a - bq - b \geq 0$$
$$\Rightarrow a - b(q + 1) \geq 0$$
$$\Rightarrow a - b(q + 1) \in S$$

But $a - b(q + 1) < a - bq$ as $b > 0$, which contradicting $r = a - bq$ is the least element of S. Therefore $r < b$. Thus $0 \leq r < b$.

Uniqueness: Suppose $a = bq + r = aq' + r', \ 0 \leq r, r' < b$

$$\Rightarrow b(q - q') = r' - r$$

Suppose $r' > r$. Then $r' - r > 0$ and $b | r' - r \Rightarrow b < r' - r$

Which is a contradiction because $r, r' < a \Rightarrow r' - r < a$.

Therefore $r' \not> r$. Similarly $r' \not< r$.

Thus given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

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

Example 1: Let $a = 25$ and $b = 4 > 0$. Then there exist unique integers $q = 6$ and $r = 1 < 4$ such that $25 = 4.6 + 1$.

Corollary 1.3.2 If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that $a = bq + r,\ 0 \le r < |b|$.

Proof: If $b > 0$, then $|b| = b$ and by theorem 1.3.1, the result holds.

If $b < 0$, then $|b| = -b > 0$. Hence by theorem 1.3.1, there exist unique integers q_1 and r such that

$$a = (-b)q_1 + r,\ 0 \le r < |b|.$$

If we take $-q_1 = q$, we get

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

Example 2: Consider $b = -7$. Then for $a = 1, -2, 61, -59$, we obtain the expressions

$$1 = (-7).0 + 1$$
$$-2 = (-7).1 + 5$$
$$61 = (-7).(-8) + 5$$
$$-59 = (-7).9 + 4$$

Example 3: Using division algorithm, show that the square of an integer leaves the remainder 0 or 1 when divided by 4.

Solution: Let a be any integer. If a is divided by 2, then possible remainders are $r = 0$ and $r = 1$, i.e., a is of the form $2q$ or $2q + 1$ for some integer q.

If $a = 2q$, then $a^2 = 4q^2$ which leaves remainder 0 when divided by 4.

If $a = 2q + 1$, then $a^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$, which leaves remainder 1 when divided by 4.

Example 4: Show that square of any odd integer is of the form $8k + 1$.

Solution: By division algorithm, any integer a is representable as one of the forms $4q, 4q + 1, 4q + 2, 4q + 3$. In this classification, only those integers of the forms $4q + 1$ and $4q + 3$ are odd.

If $a = 4q + 1$, then $a^2 = (4q + 1)^2$
$= 16q^2 + 8q + 1$
$= 8(2q^2 + q) + 1$, which is of the form $8k + 1$.

If $a = 4q + 3$, then $a^2 = (4q + 3)^2$
$= 16q^2 + 24q + 9$
$= 16q^2 + 24q + 8 + 1$
$= 8(2q^2 + 3q + 1) + 1$, which is of the form $8k + 1$.

W CHECK YOUR PROGRESS

Q.1: Show that the number of the form $\frac{a(a^2+2)}{3}$ is an integer, where a is an integer ≥ 1.

Q.2: Show that the product of any three consecutive integers is divisible by $3!$.

Q.3: If a is an odd integer, then show that $\frac{a^4+4a^2+11}{16}$ is an integer.

Q.4: If a is an odd integer, then show that $\frac{a^2+(a+2)^2+(a+4)^2}{12}$ is an integer.

1.4 GREATEST COMMON DIVISOR (GCD)

Definition 1.4.1 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 makes the statement $18 = 5c$ true.

Properties of Divisibility

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. If $a|b_k$ for $k = 1, 2, \ldots\ldots, n$, then $a|b_1x_1 + b_2x_2 + \cdots + b_nx_n$ for all integers $x_1, x_2, \ldots, x_n$.

If a and b are arbitrary integers, then an integer d is said to be a common divisor of a and b if $d|a$ and $d|b$.

Definition 1.4.2 (Greatest Common Divisor)

Let a and b be given integers with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following:

(a) $d|a$ and $d|b$.

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

Example 1: $\gcd(15, 35) = 5$, $\gcd(-8, 36) = 4$, $\gcd(-5, 5) = 5$, $\gcd(8, 17) = 1$, $\gcd(-8, -36) = 4$.

Remarks: (1) The greatest common divisor of a and b is denoted by $\gcd(a, b)$ or (a, b).

(2) $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(|a|, |b|)$.

Theorem 1.4.3 Let a and b any two integers at least one of them being non-zero. Then there exist integers x and y such that $\gcd(a,b) = ax + by$.

Proof: Let $d = \gcd(a,b)$ and $S = \{au + bv : au + bv > 0 \text{ and } u, v \in Z\}$.

Since atleast one of a or b is non-zero, so either $|a|$ or $|b|$ is in S.

If $a > 0$, then $a = a.1 + b.0 > 0 \Rightarrow a \in S$

If $a < 0$, then $-a = a.(-1) + b.0 > 0 \Rightarrow -a \in S$

Therefore $|a| \in S$, i.e., $S \neq \phi$.

By well ordering principle, S has atleast one element, say $d = au_0 + bv_0$. By definition, $d \leq |a|$ or $|b|$. By applying division algorithm to $|a|$ and d, we have

$$|a| = dq + r, \ \ 0 \leq r < d.$$

Let $r \neq 0$. Then $r = |a| - dq$

$= \pm a - q(au_0 + bv_0)$

$= a(\pm 1 - qu_0) + b(-v_0)q > 0$ and is of the form $au + bv$. Therefore $r \in S$. Also $r < d$, which contradicts the minimality of the element d in S.

Therefore $r = 0$ and then $|a| = dq \Rightarrow d||a| \Rightarrow d|a$.

Similarly, $d|b$.

If $c|a$ and $c|b$, then $c|au_0 + bv_0 = d$. Therefore $\gcd(a,b) = d = au_0 + bv_0$

Put $u_0 = x$ and $v_0 = y$, we get $\gcd(a,b) = ax + by$.

Theorem 1.4.4 Let k be any integer and a, b any integers atleast one of which is non-zero. Then $(ka, kb) = |k|(a,b)$.

Proof: Let $d = (a,b)$ and $k = (ka, kb)$. It is enough to take$k$ as positive since $(a,b) = (|a|,|b|)$.

Since $d = (a,b)$, therefore, by theorem 1.4.2, there exist integers u and v such that

$$d = au + bv$$

$$\Rightarrow dk = u(ak) + v(bk)$$

Since $t = (ka, kb)$, therefore $t|ka, t|kb \Rightarrow t|u(ka) + v(kb) \Rightarrow t|dk$ (1)

We have $d|a, d|b$

$$\Rightarrow dk|ak, dk|bk$$

$\Rightarrow dk$ is a common divisor of ak and bk.

Since $(ak, bk) = t$, therefore

$$dk|t \quad (2)$$

From (1) and (2), we obtain

$$t = dk$$

$$\Rightarrow (ka, kb) = k(a,b).$$

Corollary 1.4.5 If $(a,b)=d$, then $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

Proof: Let $(a,b)=d$, then $d|a$ and $d|b \Rightarrow a|d$ and $b|d$ are integers.
Now $d=(a,b)=\left(d.\frac{a}{d},d.\frac{b}{d}\right)=d\left(\frac{a}{d},\frac{b}{d}\right)$, using theorem 1.4.3.
Which implies $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

Definition 1.4.6 Let $a,b \in Z$ (atleast one of them being non-zero). Then we say a,b are coprime (or relatively prime) if $\gcd(a,b)=1$.

For example, (i) $\gcd(5,8)=1$, so 5 and 8 are coprime.

(ii) $\gcd(9,20)=1$, so 9 and 10 are coprime.

(iii) From corollary 1.4.4, if $(a,b)=d$, then $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.

Theorem 1.4.7 If $a|c$ and $b|c$ with $(a,b)=1$, then $ab|c$.

Proof: Let $a|c, b|c$ and $(a,b)=1$.

Now $a|c, b|c \Rightarrow c=ar,\ c=bs$ for some $r,s \in Z$.

And for $(a,b)=1$, there exist integers u,v such that

$$\begin{aligned} 1 &= au+bv \\ \Rightarrow c.1 &= c.(au+bv) \\ \Rightarrow c &= cau+cbv \\ \Rightarrow c &= bsau+arbv \\ \Rightarrow c &= ab(su+rv) \\ \Rightarrow ab|c \end{aligned}$$

Theorem 1.4.8 Let a and b be any two non-zero integers. Then a and b are relatively prime if and only if there exist integers x and y such that $ax+by=1$.

Proof: Let a and b are relatively prime. Then $(a,b)=1$.

From theorem 1.4.3, there exist x and y such that

$$\begin{aligned} (a,b) &= ax+by \\ \Rightarrow 1 &= ax+by \end{aligned}$$

Conversely, we assume $ax+by=1$ for some choice of integers x and y. Let $(a,b)=d$. Then

$$\begin{aligned} & d|a \text{ and } d|b \\ \Rightarrow\ & d|ax+by \\ \Rightarrow\ & d|1 \\ \Rightarrow\ & d=\pm 1 \\ \Rightarrow\ & d=1 \text{ as } d>0. \end{aligned}$$

Therefore $(a,b)=1$ and hence a and b are relatively prime.

Theorem 1.4.9 (Euclid's Lemma) If $a|bc$ and $(a,b)=1$, then $a|c$.

Proof: Let $a|bc$ and $(a,b)=1$. Then for $(a,b)=1$, there exist x and y in Z such that

$$1 = ax + by$$

Therefore

$$c = c.1 = c(ax + by) = cax + bcy$$

Now $a|bc$ and $a|ca \Rightarrow a|cax + bcy \Rightarrow a|c$.

W CHECK YOUR PROGRESS

Q.5: If p is a prime and a is any integer, then prove that either $p|a$ or $(a, p) = 1$.

Q.6: If p is a prime and $p|ab$, then prove that $p|a$ or $p|b$.

1.5 EUCLIDEAN ALGORITHM

The gcd of two integers a and b can be determined by a process known as Euclidean algorithm which is as follows: Let a and b be two integers such that $a \geq b > 0$. By division algorithm,

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b$$

If $r_1 = 0$, then $a = bq_1$ i.e. $b|a$ and $\gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 such that

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then we stop. When $r_2 \neq 0$, divide r_1 by r_2 to produce integers q_3 and r_3 satisfying

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say at the $(n + 1)^{th}$ stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers).

The result is the following system of equations:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 \leq r_1 < b \\
b &= r_1q_2 + r_2, \quad 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, \quad 0 \leq r_3 < r_2 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned} \qquad (*)$$

Theorem 1.5.1 The last non-zero remainder in the above algorithm is equal to $\gcd(a, b)$.

Before proof the theorem we proof the following lemma.

Lemma 1.5.2 If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof: If $d = \gcd(a, b)$, then $d|a$ and $d|b \Rightarrow d|a - bq \Rightarrow d|r$

Thus d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c|bq + r \Rightarrow c|a$.
This makes c is common divisor of a and b, so that $c \leq d$. It now follows from the definition of $\gcd(b,r)$ that $\gcd(b,r) = d = \gcd(a,b)$.

Proof of Theorem 1.5.1 Using the result of the lemma 1.5.2, from system of equations $(*)$, we obtain

$$\gcd(a,b) = \gcd(b,r_1) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n.$$

Example 1: Find $\gcd(12378,3054)$ using Euclidean algorithm.
Solution: Apply division algorithm to the numbers 12378 and 3054, we get the following equations

$$12378 = 3054 \times 4 + 162$$
$$3054 = 162 \times 18 + 138$$
$$162 = 138 \times 1 + 24$$
$$138 = 24 \times 5 + 18$$
$$24 = 18 \times 1 + 6$$
$$18 = 6 \times 3 + 0$$

Here 6 is the last nonzero remainder, therefore $\gcd(12378,3054) = 6$.

W CHECK YOUR PROGRESS

Q.7: Find $\gcd(306,657)$ and $\gcd(272,1479)$ using the Euclidean algorithm.
Q.8: Using the Euclidean algorithm to obtain integers x and y satisfying the following:
(a) $\gcd(56,72) = 56x + 72y$
(b) $\gcd(24,138) = 24x + 138y$

1.6 LEAST COMMON MULTIPLE (LCM)

Definition 1.6.1 (Least Common Multiple) The least common multiple of two non-zero integers a and b, denoted by $lcm(a,b)$, is the positive integer m satisfying the following:
(a) $a|m$ and $b|m$
(b) If $a|c$ and $b|c$ with $c > 0$, then $m \leq c$.

Remarks
(1) The least common multiple of a and b is also denoted by $[a,b]$.
(2) $lcm(a,b) \leq |ab|$ for any nonzero integers a and b.
For example, the positive common multiples of the integers -12 and 30 are $60, 120, 180, \ldots\ldots$; hence $lcm(-12,30) = 60$.

Theorem 1.6.2 Let a and b be any two positive integers. Then $\gcd(a,b).lcm(a,b) = ab$.
Proof: Let $\gcd(a,b) = d$ and $lcm(a,b) = m$.

For $\gcd(a,b)=d$, there exist integers r,s and integers u,v such that

$$a=dr,\ b=ds,\ (r,s)=1 \quad (1)$$

and $$d=au+bv \quad (2)$$

$m=lcm(a,b)$, so there exist integers t and w such that

$$m=at \text{ and } m=bw \quad (3)$$

From (2),

$$\begin{aligned} d &= au+bv \\ \Rightarrow md &= m(au+bv) \\ &= mau+mbv \\ &= bwau+atbv \\ &= ab(wu+tv) \end{aligned}$$

$$\therefore\ ab|md \quad (4)$$

Also

$$\frac{ab}{d}=\frac{drb}{d}=rb, \text{ using (1)}$$

$$\frac{ab}{d}=\frac{a.ds}{d}=as, \text{ using (1)}$$

Therefore

$$a|\frac{ab}{d} \text{ and } b|\frac{ab}{d}$$

$\Rightarrow \frac{ab}{d}$ is a common multiple of a and b

Since $lcm(a,b)=m$, so $m|\frac{ab}{d} \Rightarrow md|ab \quad (5)$

From (4) and (5),

$$md=ab$$

$$\gcd(a,b)\,.\,lcm(a,b)=ab.$$

Corollary 1.6.3 If a and b are positive integers, then $lcm(a,b)=ab \Leftrightarrow \gcd(a,b)=1$.

Example 1: $gcd(3054,12378)=6$. Find $lcm(3054,12378)$.

Solution: We have

$$\begin{aligned} \gcd(3054,12378)\,.\,lcm(3054,12378) &= 3054\times 12378 \\ \Rightarrow 6\times lcm(3054,12378) &= 3054\times 12378 \\ \Rightarrow lcm(3054,12378) &= \frac{3054\times 12378}{6}=6300402 \end{aligned}$$

Theorem 1.6.4 If $m=[a_1,a_2,\dots\dots,a_n]$, then there exists l such that $a_i|l,\ i=1,2,\dots,n$ if and only if $m|l$.

Proof: Let $m|l$. Since $m=[a_1,a_2,\dots\dots,a_n]$, so $a_i|m$ for all $i=1,2,\dots,n$.

Thus $a_i|m, m|l \Rightarrow a_i|l$ for all $i=1,2,\dots,n$.

Conversely, let $a_i|l$ for all $i=1,2,\dots,n$. We have to prove $m|l$.

If possible, let $m\nmid l$. Then by division algorithm,

$$\begin{aligned} l &= mq+r \quad (0<r<m) \\ \Rightarrow r &= l-mq \end{aligned}$$

Since $a_i|m$ and $a_i|l$, so $a_i|l-mq$ for all $i=1,2,\dots,n$

$$\Rightarrow a_i|r \text{ for all } i=1,2,\dots,n$$

But m is the least number such that $a_i|m$ for all $i = 1, 2, \ldots, n$.
Therefore, we can conclude that $m|l$.

Theorem 1.6.5 For $m > 0$, $[ma, mb] = m[a, b]$.
Proof: Let $M = [ma, mb]$. Then $ma|M$ and $mb|M$.
Therefore, we can write $M = mx$ for some integer x.
If $[a, b] = x_1$, then

$$a|x_1,\ b|x_1$$
$$\Rightarrow am|x_1m,\quad bm|x_1m$$

Since $[ma, mb] = M$, so

$$M|mx_1$$
$$\Rightarrow mx|mx_1$$
$$\Rightarrow x|x_1 \qquad (1)$$

Also $am|M$ and $bm|M \Rightarrow am|mx$ and $bm|mx$

$$\Rightarrow a|x \text{ and } b|x$$

Since $[a, b] = x_1$, so $x_1|x$ (2)
From (1) and (2), $x = x_1$
Therefore

$$M = mx_1$$
$$\Rightarrow [ma, mb] = m[a, b].$$

W CHECK YOUR PROGRESS

Q.9: Find gcd and lcm of 119 and 272.
Q.10: Find $lcm(143, 227)$, $lcm(306, 657)$.
Q.11: Find $lcm(8, 12, 15, 20, 25)$.

1.7 KRONECKER'S THEOREM

Definition 1.7.1 (Minimal Algorithm) Let a and b be positive integers and $a > b$. Then gcd of a and b can be determined by a process known as minimal algorithm which is as follows:

For two positive integers a, b and $a > b$; there exist integers Q_1 and R_1 such that

$$a = bQ_1 + e_1R_1,\ \ 0 < R_1 \leq \frac{b}{2}$$

Again, there exist integers Q_2 and R_2 such that

$$b = R_1Q_2 + e_2R_2,\ \ 0 < R_2 \leq \frac{R_1}{2}$$

Continuing this process, we get

$$R_1 = R_2Q_3 + e_3R_3,\ \ 0 < R_2 \leq \frac{R_2}{2}$$

… … … … … … … … … … … … …

… … … … … … … … … … … … …

$$R_{n-3} = R_{n-2}Q_{n-1} + e_{n-1}R_{n-1},\ \ 0 < R_{n-1} \leq \frac{R_{n-2}}{2}$$

$$R_{n-2} = R_{n-1}Q_n + e_nR_n,\ \ R_n = 0$$

Where $e_1, e_2, \ldots\ldots, e_n$ are all 1 or -1.

Since $a > b > R_1 > R_2 > \cdots > R_n$ form a decreasing sequence of non-negative integers. It follows that $R_n = 0$, for some integer n. Then $\gcd(a,b) = R_{n-1}$ as in Euclidean algorithm.

For example, consider $a = 671$ and $b = 396$.

Minimal algorithm,

$$671 = 396.2 - 121$$

$$396 = 121.3 + 33$$

$$121 = 33.4 - 11$$

$$33 = 11.3 + 0$$

Here $R_4 = 0$. Therefore $R_3 = 11 = \gcd(671, 396)$.

Euclidean algorithm,

$$671 = 396.1 + 275$$

$$396 = 275.1 + 121$$

$$275 = 121.2 + 33$$

$$121 = 33.3 + 22$$

$$33 = 22.1 + 11$$

$$22 = 11.2 + 0$$

Hence $\gcd(671, 396) = 11$.

Theorem 1.7.2 (Kronecker's Theorem)

The number of divisions in the minimal algorithm for two positive integers a and b is less than or equal to the number of divisions in Euclidean algorithm, i.e., $M(a,b) \leq E(a,b)$, where $M(a,b)$ is the number of division in minimal algorithm and $E(a,b)$ is the number of divisions in the Euclidean algorithm.

Proof: We shall prove this theorem by mathematical induction method. For $a = 2$ and $b = 1$, we have

$$2 = 1.2 + 0$$

Therefore $E(a,b) = 1 = M(a,b)$.

For $a = 3,\ b = 1$, we have $3 = 1.3 + 0$

Therefore $E(a,b) = M(a,b) = 1$.

For $a = 3,\ b = 2$, we have

$$3 = 2.1 + 1$$

$$2 = 1.2 + 0$$

Therefore $E(a,b) = 2,\ M(a,b) = 1$ and so

$$M(a,b) < E(a,b)$$

Hence the result holds for $a = 3$.

Let the theorem holds for $a = 2, 3, \ldots, k-1$. We have to prove the result holds for $a = k$. Let b be a positive integer $< k$. Then we have

$k = bQ + eR$, where $e = \pm 1$ and $0 < R \leq \frac{b}{2}$

Then

$$M(k,b) = 1 + M(b,R) \qquad (1)$$

Also

$$k = bq + r,\ \ 0 \leq r < b$$

Hence

$$E(k,b) = 1 + E(b,r) \qquad (2)$$

Now there may be three possibilities:

(i) $0 = R = r$

(ii) $0 < R = r$

(iii) $0 < R < r$

In case (i), we have $M(k,b) = E(k,b) = 1$. Therefore, the theorem holds for $a = k$.

In case (ii), $E(k,b) = 1 + E(b,R)$

But $b < k$ and $R < b$. Therefore, by assumption,

$$M(b,R) \leq E(b,R) \qquad (3)$$

From (2),

$$E(k,b) = 1 + E(b,R) \geq 1 + M(b,R) \qquad [using\ (3)]$$

$$= M(k,b)$$

In case (iii), if $0 < R < r$, then $r = b - R$.

From (2), $E(k,b) = 1 + E(b, b-R)$ (4)

Now $b < k$ and $b - R < b$, therefore by induction

$$E(b, b-R) \geq M(b, b-R) \qquad (5)$$

From (4),

$$E(k,b) = 1 + E(b, b-R)$$

$$\geq 1 + M(b, b-R)$$

$$\geq 1 + M(b, R) = M(k, b)$$

Therefore, the theorem holds for $a = k$. Hence by mathematical induction the result is true for $a > 1$.

Example: Show that $M(a, b) < E(a, b)$ for $a = 525$ and $b = 124$.

Solution: Minimal algorithm:

$$525 = 124.4 + 29 \quad 0 < 29 < \frac{124}{2}$$

$$124 = 29.4 + 8 \quad 0 < 8 < \frac{29}{2}$$

$$29 = 8.4 - 3 \quad 0 < 3 < \frac{8}{2}$$

$$3 = 1.3 + 0$$

$\therefore \; M(525, 124) = 4$ and $\gcd(525, 124) = 1$.

Euclidean algorithm:

$$525 = 124 \times 4 + 29$$

$$124 = 29 \times 4 + 8$$

$$29 = 8 \times 3 + 5$$

$$8 = 5 \times 1 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

$E(525, 124) = 7$ and $\gcd(525, 124) = 1$.

Thus

$$M(525, 124) < E(525, 124).$$

21.8 LET US SUM UP

- **Division Algorithm:** Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying $a = bq + r$, $0 \leq r < b$. The integers q and r are called respectively the quotient and remainder in the division of a by b.
- **Greatest Common Divisor:** Let a and b be given integers with atleast one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following:
  (a) $d|a$ and $d|b$
  (b) If $c|a$ and $c|b$, then $c \leq d$.

- Let a and b any two integers at least one of them being nonzero. Then there exist integers x and y such that
$$\gcd(a,b) = ax + by$$
- Let k be any integer and a, b any integers at least one of which is non-zero. Then
$$\gcd(ka, kb) = |k| \gcd(a,b)$$
- If $(a,b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
- Let $a, b \in Z$ (atleast one of them being non-zero). Then we say a, b are coprime (or relatively prime) if $\gcd(a,b) = 1$.
- If $a|c$ and $b|c$ with $(a,b) = 1$, then $ab|c$.
- Let a and b be any two non-zero integers. Then a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$.
- **Euclid's Lemma:** If $a|bc$ and $(a,b) = 1$, then $a|c$.
- The g.c.d of two integers a and b can be determined by a process known as Euclidean algorithm which is as follows:
For $a \geq b > 0$,
$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$
$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2$$
… … … … … … … … … … … … …
… … … … … … … … … … … … …
$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} + 0$$
Then $\gcd(a,b) = r_n$, the last nonzero remainder.
- **Least Common Multiple (LCM):** The least common multiple of two nonzero integers a and b, denoted by $lcm(a,b)$, is the positive integers m satisfying the following:
(a) $a|m$ and $b|m$
(b) If $a|c$ and $b|c$, with $c > 0$, then $m \leq c$.
- Let a and b be two positive integers. Then $\gcd(a,b) \,.\, lcm(a,b) = ab$.
- If $m = lcm(a_1, a_2, \dots, a_n)$, then there exist l such that $a_i|l$, $i = 1, 2, \dots, n$ if and only if $m|l$.
- For $m > 0$, $lcm(ma, mb) = m.lcm(a,b)$.
- **Minimal Algorithm:** Let a and b be positive integers and $a > b$. Then gcd of a and b can be determined by a process known as minimal algorithm which is as follows:
$$a = bQ_1 + e_1 R_1, \quad 0 < R_1 \leq \frac{b}{2}$$
$$b = R_1 Q_2 + e_2 R_2, \quad 0 < R_2 \leq \frac{R_1}{2}$$
$$R_1 = R_2 Q_3 + e_3 R_3, \quad 0 < R_2 \leq \frac{R_2}{2}$$
… … … … … … … … … … … … …

… … … … … … … … … … … … …

$$R_{n-3} = R_{n-2}Q_{n-1} + e_{n-1}R_{n-1},\ \ 0 < R_{n-1} \leq \frac{R_{n-2}}{2}$$

$$R_{n-2} = R_{n-1}Q_n + e_nR_n,\ \ R_n = 0$$

Where $e_1, e_2, \ldots\ldots, e_n$ are all 1 or -1.

Since $a > b > R_1 > R_2 > \cdots > R_n = 0$, therefore $\gcd(a, b) = R_{n-1}$.

- The number of divisions in the minimal algorithm for two positive integers a and b is less than or equal to the number of divisions in Euclidean algorithm, i.e., $M(a, b) \leq E(a, b)$.

K 1.9 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q.1: By division algorithm, every integer a is of the form $3q, 3q + 1, 3q + 2$.

Now if $a = 3q$, then

$\frac{a(a^2+2)}{3} = \frac{3q\{(3q)^2+2\}}{3} = q(9q^2 + 1)$, which is an integer.

If $a = 3q + 1$, then

$$\frac{a(a^2 + 2)}{3} = \frac{(3q + 1)\{(3q + 1)^2 + 2\}}{3}$$
$$= (3q + 1)(3q^2 + 2q + 1), \text{ which is an integer.}$$

If $a = 3q + 2$, then

$$\frac{a(a^2 + 2)}{3} = \frac{(3q + 2)\{(3q + 2)^2 + 2\}}{3}$$
$$= (3q + 2)(3q^2 + 4q + 2), \text{ which is an integer.}$$

Thus, a number of the form $\frac{a(a^2+2)}{3}$ is always an integer for a is an integer ≥ 1.

Answer to Q.2: Let $a, a + 1, a + 2$ be any three consecutive integers. Then we have to show $a(a + 1)(a + 2)$ is divisible by $3!$. We shall show this result by mathematical induction.

For $a = 1$, $a(a + 1)(a + 2) = 1.2.3 = 3!$, which is divisible by $3!$. Thus the result is true for $a = 1$.

Let the result be true for $a = k$, i.e., $k(k + 1)(k + 2)$ is divisible by $3!$. We have to prove the result is true for $a = k + 1$.

Now

$$a(a + 1)(a + 2) = (k + 1)(k + 2)(k + 3)$$
$$= k(k + 1)(k + 2) + 3(k + 1)(k + 2) \qquad (1)$$

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

Thus, $a(a+1)(a+2)$ is divisible by $3!$ for $a = k+1$, i.e., the result is true for $a = k+1$.

Hence by mathematical induction the product of any three consecutive integers is divisible by $3!$.

Answer to Q.3: Left as an exercise.

Answer to Q.4: Let a be an odd integer. Then $a = 2k+1$ for some integer k.
Now

$$\frac{a^2+(a+2)^2+(a+4)^2+1}{12}$$
$$= \frac{(2k+1)^2+(2k+1+2)^2+(2k+1+4)^2+1}{12}$$
$$= \frac{(2k+1)^2+(2k+3)^2+(2k+5)^2+1}{12}$$
$$= \frac{12k^2+36k+36}{12}$$
$$= k^2+3k+3, \text{ which is an integer.}$$

Therefore $\frac{a^2(a+2)^2+(a+4)^2+1}{12}$ is an integer for any odd integer a.

Answer to Q.5: If $p|a$, then there is nothing to prove. If $p \nmid a$, then we have to prove $(a,p) = 1$.

Let $d = (a,p)$. Then $d|a$ and $d|p$.
Since p is a prime number, this implies that $d = 1$ or $d = p$. If $d = p$, then $p|a$, which is a contradiction. Hence $d = 1$, i.e., $(a,p) = 1$.

Answer to Q.6: Let p be prime and $p|ab$. We have to prove $p|a$ or $p|b$. Let $p \nmid a$. Then $(p,a) = 1$ and there exist $x, y \in Z$ such that

$$xp + ay = 1$$
$$\Rightarrow x(bp) + y(ab) = b$$

We have

$$p|bp \text{ and } p|ab$$
$$\Rightarrow p|x(bp) + y(ab)$$
$$\Rightarrow p|b$$

Similarly, if $p \nmid b$, then $p|a$.
Hence, if p is prime and $p|ab$, then $p|a$ or $p|b$.

Answer to Q.7: Left as an exercise.

Answer to Q8: **(a)** By Euclidean algorithm,

$$72 = 56 \times 1 + 16$$
$$56 = 16 \times 3 + 8$$
$$16 = 8 \times 2 + 0$$
$$\therefore \gcd(56, 72) = 8$$
$$= 56 - 16 \times 3$$

$$= 56 - (72 - 56 \times 1) \times 3$$
$$= 56 - 72 \times 3 + 56 \times 3$$
$$= 56 \times 4 + 72 \times (-3)$$
$$= 56x + 72y \text{ where } x = 4,\ y = -3.$$

(b) Left as an exercise.

Answer to Q.9: By Euclidean algorithm,

$$272 = 119 \times 2 + 34$$
$$119 = 34 \times 3 + 17$$
$$34 = 17 \times 2 + 0$$

$\therefore \gcd(119, 272) = 17.$

We have

$$\gcd(119, 272) \times lcm(119, 272) = 119 \times 272$$
$$\Rightarrow lcm(119, 272) = \frac{119 \times 272}{\gcd(119, 272)}$$
$$= \frac{119 \times 272}{17} = 1904$$

Answer to Q.10: Left as an exercise.

Answer to Q.11: We have

$$lcm(a, b) = \frac{a \times b}{\gcd(a, b)}$$

So

$$lcm(8, 12) = \frac{8 \times 12}{\gcd(8, 12)} = \frac{8 \times 12}{4} = 24$$
$$lcm(24, 15) = \frac{24 \times 15}{\gcd(24, 15)} = \frac{24 \times 15}{3} = 120$$
$$lcm(120, 20) = \frac{120 \times 20}{\gcd(120, 12)} = \frac{120 \times 20}{20} = 120$$
$$lcm(120, 25) = \frac{120 \times 25}{\gcd(120, 25)} = \frac{120 \times 25}{5} = 600$$

Therefore $lcm(8, 12, 15, 20, 25) = 600.$

1.10 FURTHER READING

1. David M. Burton, Elementary Number Theory (7^{th} Edn.), McGraw Hill Education (India) Private Limited, Chennai-600116, 2018.

2. S. B. Malik, Basic Number Theory (2^{nd} revised Edn.), Vikash Publishing House Private Limited, Noida-201301, 2017.
3. George E. Andrews, Number Theory, Hindustan Publishing Corporation, New Delhi.
4. S. G. Telang, Number Theory, Tata McGraw-Hill Publishing Company Limited.

5. Hardy, G. H. And Wright, E. M., Theory of Numbers, Oxford Sience Publications, 2003.

M 1.11 MODEL QUESTIONS

Q.1 Use the Division Algorithm to establish the following:

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

(b) The cube of any integer has one of the forms: $9k, 9k + 1$ or $9k + 8$.

Q.2 Prove that $3a^2 - 1$ is never a perfect square.

Q.3 For $n \geq 1$, prove that $\frac{n(n+1)(2n+1)}{6}$ is an integer.

Q.4 Prove that no integer in the following sequences is a perfect square:

(a) $11, 111, 1111, \ldots\ldots\ldots\ldots$

(b) $99, 999, 9999, \ldots\ldots\ldots\ldots$

Q.5 Prove that for any integer a, one of the integers $a, a + 2, a + 4$ is divisible by 3.

Q.6 Prove that for a positive integer n and any integer a, $\gcd(a, a + n)$ divides n; hence $\gcd(a, a + 1) = 1$.

Q.7 For any integer a, show the following:

(a) $\gcd(2a + 1, 9a + 4) = 1$

(b) $\gcd(5a + 2, 7a + 3) = 1$

Q.8 If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then prove that $\gcd(a, bc) = 1$.

Q.9 If $\gcd(a, b) = 1$, then prove that $\gcd(a^2, b^2) = 1$.

Q.10 If $a > 1$ and m, n are positive integers, then $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

Q.11 Use the Euclidean algorithm to obtain integers x and y satisfying the following:

(a) $\gcd(119, 272) = 119x + 272y$

(b) $\gcd(1769, 2378) = 1769x + 2378y$.

Q.12 Assuming that $\gcd(a, b) = 1$. Prove the following:

(a) $fcd(a + b, a - b) = 1$ or 2

(b) $\gcd(2a + b, a + 2b) = 1$ or 3.

Q.13 Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

Q.14 Given non-zero integers a and b, prove that $\gcd(a, b) = lcm(a, b)$ if and only if $a = \pm b$.

*** *** ***