Number Theory and Graph Theory

Chapter 1

Introduction and Divisibility

By

A. Satyanarayana Reddy

Department of Mathematics

Shiv Nadar University

Uttar Pradesh, India

E-mail: satya8118@gmail.com

Module-2: Properties of division of integers and Division algorithm

Objectives

- Division and its properties.
- Division Algorithm and its applications.

1 Division and its Properties

Definition 1.1. *Let $a, b \in \mathbb{Z}$ and $a \neq 0$. Then a is said to divide b if there is an integer k such that $b = ak$. We denote it by $a \mid b$ and $a \nmid b$ means that a does not divide b.*

Remark 1.2. *$a \mid b$ is a statement, for example $2|6$ is true, and $6|2$ is false. Where as $\frac{6}{2}$ is a number equal to 3.*

Following properties are easy to verify, hence we state them without proof.

Theorem 1.3 (Few properties of division)**.** *Let a, b, and d be integers. Then, the following statements hold:*

Reflexive property: *$a \mid a$ (every integer divides itself).*

Transitivity property: *$d \mid a$ and $a \mid b \implies d \mid b$.*

Linearity Property: *$d \mid a$ and $d \mid b \implies d \mid an + bm$ for all n and m.*

That is if $d|a, b$, then d divides every integer linear combination of a and b.

Cancellation Property: *$ad \mid an$ and $a \neq 0 \implies d \mid n$.*

Multiplication Property: *$d \mid n \implies ad \mid an$.*

1 and -1 divides every integer: $1 \mid n, -1 \mid n \;\; \forall n \in \mathbb{Z}$.

1 and -1 are divisible by 1 and -1 only: $n \mid 1 \Longrightarrow n = \pm 1$.

Another equivalent way of stating the above two properties is: 1 *and* -1 *are the only invertible elements in* $\mathbb{Z}$.

Every number divides zero: $d \mid 0 \;\; \forall d \in \mathbb{Z}$.

Comparison Property: *If d and n are positive and $d \mid n$ then $d \leq n$.*

2 Division Algorithm

One of the important application of WOP is the division algorithm.

Suppose an integer a is divided by an integer $b \neq 0$. Then we get a unique quotient q and a unique remainder r, where the remainder satisfies the condition $0 \leq r < |b|$. Here a is the dividend and b the divisor.

This is just saying another way that either a is multiple of b or a lies between two multiples of b.

This is formally stated as follows.

Theorem 2.1 (Division Algorithm)**.** *Let $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$. Then there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$, where $0 \leq r < |b|$.*

Proof. **Existence:** First we prove the result when b is positive *i,e.,* $b \geq 1$.

- Consider the set $S = \{a - bn | n \in \mathbb{Z}\}$. That is $S = \{a, a \pm b, a \pm 2b, a \pm 3b, \ldots, \}$. It is clear that S contains infinitely many integers. Further, when $n = -|a|$ we have $a - b(-|a|) = a + b|a| \geq a + |a| \geq 0$. Thus, S contains non negative integers.

- Let $S' = S \cap (\mathbb{N} \cup \{0\})$. Then, by the Well-ordering principle S' has a least element, say r. Now we have $r \in S' \subseteq S$, hence there exists a $q \in \mathbb{Z}$ such that $r = a - bq$ or $a = bq + r$. And also from definition of S', we have $0 \leq r$.
- Now we will show that $r < b$. Suppose $r \geq b$, then $0 \leq r - b = a - bq - b = a - b(q+1) \in S'$ and $r - b < r$ (as $b \geq 1$) which is a contradiction as r is the least element in S'.

Uniqueness: Let $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $a = bq_1 + r_1 = bq_2 + r_2$, where $0 \leq r_1 < b$ and $0 \leq r_2 < b$.

claim: $r_1 = r_2$ **and** $q_1 = q_2$

Suppose $r_1 \geq r_2$. Then

$$r_1 - r_2 \in \{0 \cdot b, 1 \cdot b, 2 \cdot b, \ldots\},$$

as $r_1 - r_2 = b(q_2 - q_1)$. Thus, b divides $r_1 - r_2$ and $0 \leq r_1 - r_2 \leq r_1 < b$. Which is possible only if $r_1 - r_2 = 0$ and hence, $q_1 - q_2 = 0$.

If b is negative, then $-b$ is positive, hence there exists $q, r \in \mathbb{Z}$ such that $a = (-b)q + r = b(-q) + r$, where $0 \leq r < -b$.

□

2.1 Few applications of Division Algorithm

b=2: Let a be any integer. Then, by division algorithm $a = bq + r$ where $r = 0$ or $r = 1$. That is, the only possible remainders are $r = 0$ or $r = 1$. When $r = 0$, we have $a = 2q$, called an even integer. When $r = 1$, $a = 2q + 1$, called an odd integer.

b=3: Then, the possible remainders are $r = 0$ or 1 or 2. Consequently, every integer can be expressed as $3q$ or $3q + 1$ or $3q + 2$. In other words, $\mathbb{Z} = \{3q | q \in \mathbb{Z}\} \cup \{3q + 1 | q \in \mathbb{Z}\} \cup \{3q + 2 | q \in \mathbb{Z}\}$.

b=4: We have $\mathbb{Z} = \{4q|q \in \mathbb{Z}\} \cup \{4q+1|q \in \mathbb{Z}\} \cup \{4q+2|q \in \mathbb{Z}\} \cup \{4q+3|q \in \mathbb{Z}\}$.

The advantage of division algorithm is that it allows us to prove assertions about all the integers by considering only a finite number of cases. For example,

Let a be any integer. Then $a = 2q$ or $a = 2q+1$ so that $a^2 = 4k$ or $a^2 = 4k+1$. **In other words, square of an integer can not be of the form** $4k+2$ **or** $4k+3$.

Similarly, one can prove that **a square odd integer must have the form** $8k+1$**, for some integer** k.

Proof. Note that every odd integer has one of the forms $8k+1$ or $8k+3$ or $8k+5$ or $8k+7$. In each case, it can be easily verified that their square has the form $8q+1$. □

Problem 2.2. 1. *No integer in the following sequence is a perfect square* $\{11, 111, 1111, 11111, \ldots\}$.

Proof. We already know that the square of any integer is either of the form $4r$ or $4r+1$.

An arbitrary number of the form $1111\ldots1111 = 1111\ldots1108+3$ and 4 divides $1111\ldots1108$. Thus, all the numbers are of the form $4k+3$. Hence, they cannot be perfect squares. □

2. *Show that each term of the sequence* $16, 1156, 111556, 11115556, \ldots$ *is a perfect square.*

Proof. Let t_n be its n^{th} term. Then $t_n - 1 = R_n 10^n + 5R_n = R_n(10^n+5)$, where $R_k = \frac{10^k-1}{9}$. Note that R_k is a positive integer for all $k \in \mathbb{N}$.

$$\begin{aligned} t_n &= R_n 10^n + 5R_n + 1 = R_n(9R_n+1) + 5R_n + 1 \\ &= 9R_n^2 + 6R_n + 1 = (3R_n+1)^2 \end{aligned}$$

□

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

Proof. **If n=6k,** then $n(n+1)(2n+1) = 6k(6k+1)(12k+1)$.

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

If n=6k+2, then $n(n+1)(2n+1) = (6k+2)(6k+3)(12k+5) = 6(3k+1)(2k+1)(12k+5)$.

If n=6k+3, then $n(n+1)(2n+1) = (6k+3)(6k+4)(12k+7) = 6(2k+1)(3k+2)(12k+7)$.

If n=6k+4, then $n(n+1)(2n+1) = (6k+4)(6k+5)(12k+9) = 6(3k+2)(6k+5)(4k+3)$.

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

□

Theorem 2.3 (Pigeonhole Principle)**.** *If m pigeons are assigned to n pigeonholes, where $m > n$, then at least two pigeons must occupy the same pigeonhole.*

Proof. (by contradiction) Suppose the given conclusion is false, that is, no two pigeons occupy the same pigeonhole. Then every pigeon must occupy a distinct pigeonhole, so $n \geq m$, which is a contradiction. Thus, two or more pigeons must occupy the same pigeonhole. □

Example 2.4. *Let n be an integer ≥ 2. Suppose $n+1$ integers are selected randomly. Prove that the difference of two of them is divisible by n.*

Proof. Let q be the quotient and r the remainder when an integer a is divided by n. Then, by division algorithm, $a = nq + r$, where $0 \leq r < n$. The $n+1$ integers yield $n+1$ remainders (pigeons), but there are only n possible remainders (pigeonholes). Therefore, by the pigeonhole principle, two of the remainders must be equal.

Let x and y be the corresponding integers. Then $x = nq_1 + r$ and $y = nq_2 + r$ for some quotients q_1 and q_2. Therefore, $x - y = (nq_1 + r) - (nq_2 + r) = n(q_1 - q_2)$. Thus, $x - y$ is divisible by n. □