Number Theory

NPTEL - II Web Course

Anupam Saikia
Department of Mathematics
Indian Institute of Technology Guwahati

Contents

Notation

$\mathbb{N}$: the set of natural numbers, i.e., $\{1,\ 2,\ \cdots\}$

$\mathbb{Z}$: the set of integers, i.e., $\{0,\ \pm 1,\ \pm 2,\ \cdots\}$

$\mathbb{Q}$: the set of rational numbers, i.e., $\{\frac{m}{n}\ \mid\ m,\ n \in \mathbb{Z},\ n \neq 0\}$

$\mathbb{R}$: the set of real numbers

For a real number x, $\mid x \mid$ denotes the absolute value of x, i.e.,
$\mid x \mid = x$ if $x \geq 0$ and $\mid x \mid = -x$ if $x < 0$.

#S: the number of elements is a set S.

$Re(s)$: the real part of a complex number s.

Module 1

Divisibility and Primes

1.1 Lecture 1

Preamble: In this lecture, we will look into the notion of divisibility for the set of integers. Then we will discuss the division algorithm for integers, which is crucial to most of our subsequent results.

Keywords: divisibility, well-ordering principle, induction, division algorithm.

1.1.1 Introduction

We will start by discussing the notion of divisibility for the set $\mathbb{Z}$ of integers. We will be frequently using the fact that both addition and multiplication in $\mathbb{Z}$ are associative, commutative and we also have distributivity property $a(b+c) = ab+ac$ for any integers a, b, c. These operations give the structure of a commutative ring to the set $\mathbb{Z}$. Divisibility can be studied more generally in any commutative ring, for example, the ring of polynomials with rational coefficients. However, you need not be familiar with concepts of ring theory to understand these lectures as our focus will be on integers.

Definition 1.1. *If a and $b \neq 0$ are integers and $a = qb$ for some integer q, then we say that b divides a, or that a is a multiple of b, or that b is a factor/divisor of a. If b divides a, we denote it by $b \mid a$, and if b does not divide a we denote it by $b \nmid a$.*

For example, $6 \mid 36$ but $7 \nmid 36$. Note that $b \mid 0$ for any non-zero integer b and $1 \mid a$

for any integer a. When we write $b \mid a$, it is tacitly assumed that b is a non-zero integer. We can easily deduce the following properties from the definition of divisibility itself.

PROPOSITION 1.2. *Let a, b, c d be any non-zero integers.*

1. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*
2. *If $a \mid b$ and $c \mid d$ then $ac \mid bd$.*
3. *If m is a non-zero integer then $a \mid b$ if and only if $ma \mid mb$.*
4. *If d is a non-zero integer such that $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.*
5. *If a divides x and y then a divides $cx + dy$ for any integers c, d.*
6. *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Proof: 1. Suppose $b = na$ and $c = mb$, where $n,\ m \in \mathbb{Z}$. Then $c = m(na) = (mn)a$ and so $a \mid c$.

2. Suppose $b = na$ and $d = mc$ where $n,\ m \in \mathbb{Z}$. Then $bd = (na)(mc) = (mn)(ac)$, i.e., $ac \mid bd$.

3. Suppose $b = na$. Then $mb = m(na) = n(ma)$ and $ma \mid mb$. Conversely, let $mb = d(ma) = m(da)$. Then $m(b - da) = 0$. But $m \neq 0$, hence $b = da$, i.e., $b \mid a$.

4.

$$\begin{aligned} a = dq &\implies |a| = |dq| = |d|\ |q| \\ a \neq 0 \implies q \neq 0 &\implies |a| = |d|\ |q| \geq |d|. \end{aligned}$$

5.

$$\begin{aligned} x = an, &\qquad y = am \\ \implies cx + dy &= c(an) + d(am) \\ &= a(cn + dm). \end{aligned}$$

6. By (4) above,

$$\begin{aligned} a \mid b &\implies |a| \leq |b|, \\ b \mid a &\implies |b| \leq |a| \\ &\implies |a| = |b|, \\ &\implies a = \pm b. \qquad \square \end{aligned}$$

1.1.2 Well-ordering Principle

We begin this section by mentioning the well-ordering principle for non-negative integers.

Well-ordering Principle: *If S is a non-empty set of non-negative integers, then S has a least element, i.e., there is an integer $c \in S$ such that $c \leq x$ for all $x \in S$.*

The principle of mathematical induction follows directly from well-ordering principle. We will use the principle of induction in several arguments later.

THEOREM 1.3. (Principle of Induction): *Let S be set of positive integers such that*

1. $1 \in S$
2. $k \in S \implies k+1 \in S$

Then S is the the set $\mathbb{N}$ of all natural numbers.

Proof: Consider the complement S' of the set S in $\mathbb{N}$:

$$S' = \mathbb{N} - S.$$

We want to show that S' is the empty set. Suppose S' is non-empty. Then by well-ordering principle it has a least element, say n'. Clearly, $n' \neq 1$ as $1 \in S$. Therefore $n' - 1$ is a natural number which is not in S'. Hence $n' - 1 \in S$. By hypothesis, $n' - 1 \in S \implies n' \in S$. Therefore, $n' \in S \cap S'$, which is a contradiction. Therefore S' must be empty, and $S = \mathbb{N}$. $\square$

There is a stronger form of the principle of induction. The stronger version says that if $S \subset \mathbb{N}$ such that

1. $1 \in S$ and
2. $1, 2, \cdots, k \in S$ implies $k+1 \in S$ for any natural number k,

then $S = \mathbb{N}$. It is an easy exercise to see that both the versions are equivalent. We often use the induction principle in the following way. If a mathematical statement is (i) valid for $k = 1$, and (ii) valid for $k+1$ if it is valid for k (for all positive integers from 1 to k in the stronger version), then the statement is valid for all positive integers.

Example: Show that $3^n \geq 2n+1$ for all natural number n.

Proof: Clearly the statement is true for $n = 1$. Suppose it is true for $n = k$. Then,

$$\begin{aligned} 3^{k+1} &= 3 \cdot 3^k \\ &\geq 3 \cdot (2k+1) = 6k+3 \\ &> 2k+3 = 2(k+1)+1. \end{aligned}$$

Thus the statement hold for $k+1$ if it hold for k. Hence the statement holds for all integers n. $\square$

1.1.3 Division Algorithm

The division algorithm for integers is a fundamental property that we will utilize time and again. The division algorithm follows from the well-ordering principle. It can be stated as follows:

THEOREM 1.4. *If a ad b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that*

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

Proof: First assume that $b > 0$. Let

$$S = \{a - nb \mid n \in \mathbb{Z}, \;\; a - nb \geq 0\}.$$

The set S is clearly non-empty, as it contains the element

$$a + |a|b \geq a + |a| \geq 0 \qquad (\text{with } n = -|a|).$$

By the well-ordering principle, S has a least element r so that $r = a - qb$ for some integer q. So we have $a = qb + r$ with $r \geq 0$. It is now enough to show that $r < b$. If $r \geq b$, then $r - b = a - (q+1)b \geq 0$ and $r - b$ is also contained in S, which contradicts the fact that r is the least element of S. Hence, we must have $0 \leq r < b$.

To prove uniqueness, suppose $a = qb + r = q_1 b + r_1$ with $0 \leq r < b$ and $0 \leq r_1 < b$. If $q \neq q_1$, we can assume $q > q_1$ without loss of generality. Then, $r - r_1 = (q - q_1)b \geq 1 \cdot b = b$. But r and r_1 are both non-negative and are strictly less than b, hence $r - r_1$ can not be bigger than b. So, $q = q_1$ and hence $r = r_1$.

For the case $b < 0$, simply apply the result for $-b$ to obtain unique integers q and r such that $a = q(-b) + r = (-q)b + r$ where $0 \leq r < -b = |b|$. $\square$

For example, with $a = 54$ and $b = -24$, we have

$$54 = (-2)(-24) + 6, \text{ with } 0 \leq 6 < |-24|.$$

Application: If n is the square of an odd integer, then n leaves the remainder 1 when divided by 8, i.e., a perfect odd square must be of the form $8k + 1$.

Proof: Let $n = (2a+1)^2 = 4a^2 + 4a + 1 = 4a(a+1) + 1$. Now one of a or $a+1$ must be even, hence $n = 8k + 1$ for some integer k. $\square$