

Math 220

Lecture 1

Baili Min

July 13, 2009

Number Theory

Numbers like 1, 2, 0, -1, -99, ... are called integers. The set of all integers is denoted as \mathbb{Z} .

An interesting subset of \mathbb{Z} is the collection of all those positive numbers in \mathbb{Z} , denoted as \mathbb{N} . For example, 1, 4, 8, 9999999, ...

There are two important sets you should know:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$$

$$\mathbb{R} = \{\text{all real numbers}\}$$

Questions: Can you give some examples which are in \mathbb{Q} but not in \mathbb{N} ? How about examples which are in \mathbb{R} but not in \mathbb{Q} ?

Now we focus on \mathbb{Z} .

Divisibility

In \mathbb{Z} , we can do addition: $8 + 2 = 10$; subtraction: $8 - 2 = 6$ and multiplication: $8 \times 2 = 16$, and sometimes we can do division: $8 \div 2 = 4$.

Question: Can we always do division?

Definition 0.1. Suppose $a, b \in \mathbb{Z}$ and $b \neq 0$. If there exists $c \in \mathbb{Z}$ such that $a = bc$, we say b divides a , denoted by $b \mid a$, and we say b is a factor of a while a is a multiple of b .

If there does not exist such an integer c , we say b does not divide a , with the notation $b \nmid a$.

Examples:

In the exercise, you will show some basic properties of the divisibility.

One important result is called the division algorithm.

Theorem 0.2. Suppose $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exist integers q, r such that $a = bq + r$ where $0 \leq r < |b|$, and q, r are uniquely determined by the previous condition.

Examples:

The Greatest Common Divisor

Question: Can you find a common divisor for 3, 6, and 9?

Definition 0.3. Suppose a, b, \dots, c are (finitely many) integers of which at least one of them is nonzero. The (unique) integer d is called their greatest common divisor, with the notation $d = (a, b, \dots, c)$ if d satisfies the following conditions:

(i) $d|a, d|b, \dots, d|c$, and

(ii) d is the greatest, that is, if there is another integer d_1 with $d_1|a, d_1|b, \dots, d_1|c$, then we must have $d_1 \leq d$.

Question: For any group of integers, can we always find a common divisor?

Question: Must the greatest common divisor be positive?

Definition 0.4. Coprime: If $(a, b, \dots, c) = 1$, we say a, b, \dots, c are coprime.

Pairwise Coprime: For integers a, b, \dots, c , if any two of them are coprime, we say a, b, \dots, c are pairwise coprime.

You will show some properties in the exercise.

One important property is the famous Bezout Equality:

Theorem 0.5. Suppose a, b, \dots, c are (finitely many) integers of which at least one of them is nonzero, then there exist integers x, y, \dots, z such that

$$ax + by + \dots + cz = (a, b, \dots, c).$$

In particular, if a, b, \dots, c are coprime, then there exist integers x, y, \dots, z such that

$$ax + by + \dots + cz = 1.$$

Question: How to find the greatest common divisor?

The following properties will help:

Theorem 0.6. Suppose a, b, \dots, c are (finitely many) integers of which at least one of them is nonzero, and $d = (a, b, \dots, c)$, then

(i) if d_1 is another common divisor, then $d_1|d$;

(ii) $(a, b, \dots, c) = ((a, b), \dots, c)$;

(iii) Suppose $m \in \mathbb{N}$, then $(ma, mb, \dots, mc) = m(a, b, \dots, c)$;

(iv) $(\frac{a}{d}, \frac{b}{d}, \dots, \frac{c}{d}) = 1$;

(v) If $(a, m) = (b, m) = \dots = (c, m) = 1$, then $(ab \dots c, m) = 1$;

(vi) If $c|ab$ and $(c, b) = 1$, then $c|a$.

Question: Can you give some examples?

Now we can learn how to find the greatest common divisor.

From the previous theorem we can see that this problem can be reduced to find the greatest common divisor of two integers.

Question: Why?

Euclidean Algorithm:

Suppose $a, b \in \mathbb{Z}$ and $b \neq 0$, apply the division algorithm in the following way, then after finitely many steps it must stop, that is, the remainder is 0.

Divide a by b : $a = bq_0 + r_0, 0 < r_0 < |b|$;

Divide b by r_0 : $b = r_0q_1 + r_1, 0 < r_1 < r_0$;

Divide r_0 by r_1 : $r_0 = r_1q_2 + r_2, 0 < r_2 < r_1$;

\vdots

Divide r_{n-2} by r_{n-1} : $r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}$;

Divide r_{n-1} by r_n : $r_{n-1} = r_nq_{n+1}$.

Then $(a, b) = r_n$

Examples: