Elementary Number Theory **Mathematics Dept.,**
Course I - High Diploma Students **Edu. College for Pure Sciences**
Asst. Prof. Dr. Ruma Kareem K. Ajeena **University of Babylon**
ruma.usm@gmail.com

Lecture 1: Divisibility Theory in the Integers

1.1 Introduction

A short way to determine the divisibility of a given integer by a fixed divisor without performing the division can be done through examining its digits. However, there are divisibility tests for numbers to do that. In this lecture, several concepts related to the divisibility theory are discussed as follows:

1.2 The Division Algorithm

In this section, the division algorithm has been discussed as follows:

Theorem 1.2.1. (Division Algorithm). For given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

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

The integers q and r are called, respectively, the *quotient* and *remainder* in the division of a by b.

Proof. First, it requires to prove that the set

$$S = \{a - xb \mid x \text{ an integer}; a - xb \ge 0\}$$

is nonempty. For performing that, it suffices to exhibit a value of x making $a - xb$ nonnegative.

Because the integer $b \ge 1$, therefore $|a|\, b \ge |a|$, and so

$$a - (-|a|)b = a + |a|\, b \ge a + |a| \ge 0$$

For the choice $x = -|a|$, then, $a - xb$ lies in S. This paves the way for an application of the Well-Ordering Principle which states [Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that a ≤b for all b's belonging to S], this means that the set S contains a smallest integer; suppose it r. By the definition of S, there exists an integer q satisfying

$$r = a - qb \qquad 0 \le r$$

We argue that $r < b$. If this were not the case, then $r \ge b$ and

$$a - (q + 1)b = (a - qb) - b = r - b \geq 0$$

The implication is that the integer $a - (q + 1)b$ has the proper form to belong to the set S. But $a - (q + 1)b = r - b < r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r < b$.

Next, it turns to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form, say,

$$a = qb + r = q'b + r'$$

where $0 \leq r < b, 0 \leq r' < b$. Then $r' - r = b(q - q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$| r' - r | = b | q - q' |$$

Upon adding the two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we obtain $-b < r' - r < b$ or, in equivalent terms, $| r' - r | < b$. Thus, $b | q - q' | < b$, which yields

$$0 \leq | q - q' | < 1$$

Because $| q - q' |$ is a nonnegative integer, the only possibility is that $| q - q' | = 0$, whence $q = q'$; this, in turn, gives $r = r'$, ending the proof. ■

A more general version of the Division Algorithm is obtained by replacing the restriction that b must be positive by the simple requirement that $b \neq 0$.

Corollary 1.2.1. If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that

$$a = qb + r, \quad 0 \leq r < | b |.$$

Proof. It is enough to consider the case in which b is negative. Then $b > 0$, and Theorem 2.1 produces unique integers q' and r for which

$$a = q' | b | + r \quad 0 \leq r < | b |$$

Noting that $| b | = -b$, we may take $q = -q'$ to arrive at $a = qb + r$, with $0 \leq r < | b |$. ■

To illustrate the Division Algorithm when $b < 0$, let us take $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59, the following

expressions are obtained

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

1.3. The Greatest Common Divisor

On the Division Algorithm, a special significance is the case that the remainder in the turns out to be zero. This case has been presented as follows.

Definition 1.3.1 An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. It can be written a not divide b to indicate that b is not divisible by a.

Some consequences of (Definition 1.3.1) can be listed by

Theorem 1.3.1 For integers a, b, c, the following hold:

(a) a|0,1|a, a|a.

(b) a|1 if and only if a =±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 =± b.

(f) If a|b and b ≠ 0, then |a|≤|b|.

(g) If a|b and a|c, then a|(bx+cy) for arbitrary integers x and y.

Proof. The proof of the statements (f) and (g) are done as follows. (for other parts, they leave as an exercise). If a|b, then there exists an integer c such that b =ac; also, b ≠0 implies that c ≠0. By taking the absolute values, one can get

$$|b| = |ac| = |a||c|.$$

Because c ≠0, it follows that |c|≥1, whence |b|=|a||c|≥|a|.

As regards (g), the relations a|b and a|c ensure that b =ar and c =as for suitable integers r and s. With the choice of x and y, one can write the relation

$$bx + cy = arx + asy = a(rx + sy).$$

Because $rx+sy$ is an integer, this means that $a|(bx+cy)$, as desired. ■

It is worth pointing out that property (g) of Theorem (1.3.1) extends $k = 1,2,...,n$, then $a|(b_1x_1 + b_2x_2 + \cdots + b_nx_n)$ for all integers $x_1, x_2, ..., x_n$.

If a and b are arbitrary integers, then an integer d is said to be a common divisor of a and b if both $d|a$ and $d|b$. Because 1 is a divisor of every integer, 1 is a common divisor of a and b; hence, their set of positive common divisors is nonempty. Now every integer divides zero, so that if $a = b = 0$, then every integer serves as a common divisor of a and b. In this instance, the set of positive common divisors of a and b is infinite. However, when at least one of a or b is different from zero, there are only a finite number of positive common divisors. Among these, there is a largest one, called the greatest common divisor of a and b. The frame of this is given in the following Definition (1.3.2).

Definition 1.3.2 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:

(1) $d \mid a$ and $d \mid b$.

(2) if $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 1.3.1 The positive divisors of - 12 are 1, 2, 3, 4, 6, 12, whereas those of 30 are 1,2,3,5,6,10,15,30, hence, the positive common divisors of 12 and 30 are 1, 2, 3, 6. Because 6 is the largest of these integers, it follows that $\gcd(12, 30) = 6$.

In the same way, it can show that

$$\gcd(-5, 5) = 5 \qquad \gcd(8, 17) = 1 \qquad \gcd(-8, -36) = 4$$

The next theorem indicates that $\gcd(a, b)$ can be represented as a linear combination of a and b. (By a *linear combination* of a and b, we mean an expression of the form $ax + by$, where x and y are integers.)

This is illustrated by, say,

$$\gcd(-12, 30) = 6 = (-12)2 + 30 \cdot 1$$

or

$\gcd(-8, -36) = 4 = (-8)4 + (-36)(-1)$.

Now for the theorem.