Based on K. H. Rosen: Discrete Mathematics and its Applications.

Lecture 14: The Division Algorithm. Section 4.1

1 The division algorithm

We are going to do some work in the ring $\mathbb{Z}$ of integers.

1.1 Division

Definition 1. If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a **factor or divisor** of b, and that b is a **multiple** of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Remark 2. Given positive integers d and n, there are exactly $\lfloor \frac{n}{d} \rfloor$ numbers less or equal than n that are divisible by d, they are $d, 2d, 3d, \ldots, kd$ where $k = \lfloor \frac{n}{d} \rfloor$.

Properties of integer divisibility:

1. $a \mid b$ and $a \mid c \Rightarrow a \mid (b + c)$.
2. $a \mid b \Rightarrow a \mid (bc)$ for all integers c.
3. $a \mid b$ and $b \mid c \Rightarrow a \mid c$.
4. $a \mid b$ and $a \mid c \Rightarrow a \mid (mb + nc)$ for any integers m, n.

1.2 The division algorithm

When an integer is divided by a positive integer, there is a **quotient** and a **remainder**, as the division algorithm shows.

Theorem 3. *(THE DIVISION ALGORITHM) Let a be an integer and d a positive integer. Then there are unique integers q and r with $0 \leq r < d$, such that $a = dq + r$.*

Definition 4. In the equality given in the division algorithm, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**. This notation is used to express the quotient and remainder:

$$q = a \text{ div } d \qquad\qquad r = a \bmod d.$$

Remark 5. Suppose that a is an integer and b a positive integer and we write

$$a = bq + r.$$

If the integer c divides a and b, then by properties of division, it would divide also $r = a - bq$. In other words, any integer that is a common divisor of two numbers a, b $(b > 0)$, is also a divisor of the remainder of the division r of a by b.

1.3 Modular arithmetic

In some situations we care only about the remainder of an integer when it is divided by some specified positive integer.

Definition 6. If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation

$$a \equiv b \pmod{m}$$

to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a congruence and that m is its modulus (plural moduli). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$

Theorem 7. *Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.*

Proof. If $a \equiv b \pmod m$, by the definition of congruence, we know that $m \mid (a - b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$. Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod m$. □

Theorem 8. *Let m be a positive integer.*

$$If a \equiv b \pmod{m} \; and \;\; c \equiv d \pmod m \;\; then \;\; a + c \equiv b + d \pmod{m})$$

$$If a \equiv b \pmod{m} \; and \;\; c \equiv d \pmod m \;\; then \;\; ac \equiv bd \pmod{m}$$

Proof. We use a direct proof. Since we have If $a \equiv b \pmod{m}$ and $c \equiv d \pmod m$, there are integers s and t such that $b = a + sm$ and $d = c + tm$. Hence,

$$b + d = a + c + m(t + s) \text{ and } bc = ac + m(at + cs + stm)$$

and therefore

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

□

We can define arithmetic operations on $\mathbb{Z}_m$, the set of nonnegative integers less than m, that is, the set $\{1, 2, 3, \ldots, m - 1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

$$a +_m b = (a + b) \mod m,$$

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by $\cdot_m$by

$$a \cdot_m b = (a \cdot b) \mod m.$$

Properties of the modular operations:

1. (Closure) If $a, b \in \mathbb{Z}_m$, then $a +_m b, a \cdot_m b \in \mathbb{Z}_m$.

2. (Associativity) for $a, b, c \in \mathbb{Z}_m$ we have

$$(a +_m b) +_m c = a +_m (b +_m c) \qquad \text{and} \qquad (a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$$

3. (Commutativity) If $a, b \in \mathbb{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

4. (Identity elements) The element $0 \in \mathbb{Z}_m$ is the identity element for addition and 1 is the identity element for multiplication. In other words, if $a \in \mathbb{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

5. (Additive inverses) If $a \in \mathbb{Z}_m$, then we have an additive inverse

$$a +_m (m - a) = 0 \text{ for } a \neq 0 \qquad \text{and} \qquad 0 +_m 0 = 0.$$

6. (Distributivity) for $a, b, c \in \mathbb{Z}_m$ we have

$$a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c \qquad \text{and} \qquad (a +_m b) \cdot_m c = a \cdot_m c +_m b \cdot_m c.$$

Remark 9. Because $\mathbb{Z}_m$ with the operations of addition and multiplication modulo m satisfies the properties listed, $\mathbb{Z}_m$ with modular addition is said to be a **commutative group** and $\mathbb{Z}_m$ with both of these operations is said to be a **commutative ring with unit**. Note that the set of integers with ordinary addition and multiplication also forms a commutative ring.