Lecture 14

Topics:

1. Divisibility
2. Modular Arithmetic
3. Congruence Relation

4.1 Divisibility and Modular Arithmetic

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.

Example 1: Determine whether $3 \mid 7$ and whether $3 \mid 12$. Solution: We see that $3 \nmid 7$, because $\frac{7}{3}$ is not an integer. On the other hand, $3 \mid 12$ because $\frac{12}{3} = 4$.

Example 2: Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution: The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leq n$, or with $0 < k \leq \frac{n}{d}$. Therefore, there are $\left\lfloor \frac{n}{d} \right\rfloor$ positive integers not exceeding n that are divisible by d.

4.1 Divisibility and Modular Arithmetic (Continued)

THEOREM 1: Let a, b, and c be integers, where $a \neq 0$. Then (i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$; (ii) if $a \mid b$, then $a \mid bc$ for all integers c; (iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: We will give a direct proof of (i). Suppose that $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$. Hence, $b + c = as + at = a(s + t)$. Therefore, a divides $b + c$. This establishes part (i) of the theorem. The proofs of parts (ii) and (iii) are left as Exercises 3 and 4.

4.1 Divisibility and Modular Arithmetic (Continued)

COROLLARY 1: If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Proof: We will give a direct proof. By part (ii) of Theorem 1 we see that $a \mid mb$ and $a \mid nc$ whenever m and n are integers. By part (i) of Theorem 1 it follows that $a \mid mb + nc$.

4.1.3 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 2: 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 2: 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: $q = a \operatorname{div} d, \quad r = a \bmod d$.

4.1.3 The Division Algorithm (Continued)

Example 3: What are the quotient and remainder when 101 is divided by 11?

Solution: We have $101 = 11 \cdot 9 + 2$. Hence, the quotient when 101 is divided by 11 is $9 = 101 \operatorname{div} 11$, and the remainder is $2 = 101 \bmod 11$.

Example 4: What are the quotient and remainder when -11 is divided by 3?

Solution: We have $-11 = 3(-4) + 1$. Hence, the quotient when -11 is divided by 3 is $-4 = -11 \operatorname{div} 3$, and the remainder is $1 = -11 \bmod 3$. Note that the remainder cannot be negative. Consequently, the remainder is not -2, even though $-11 = 3(-3) - 2$, because $r = -2$ does not satisfy $0 \leq r < 3$. ◂

Note that the integer a is divisible by the integer d if and only if the remainder is zero when a is divided by d.

4.1.4 Modular Arithmetic

Definition 3: 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 (pl. moduli). If a and b are not congruent modulo m, we write $a \not\equiv b \ (mod\ m)$. Although both notations $a \equiv b \ (mod\ m)$ and $a \bmod m = b$ include "mod", they represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function. However, the relation $a \equiv b \pmod{m}$ and the $\bmod m$ function are closely related, as described in Theorem 3.

THEOREM 3: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

4.1.4 Modular Arithmetic (Continued)

Example 5: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution: Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$.

THEOREM 4: 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 (Definition 3), 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 $a \equiv b \pmod{m}$.

4.1.4 Modular Arithmetic (Continued)

THEOREM 5: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof: We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence, $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$. Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Example 6: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$ and that $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$.

4.1.4 Modular Arithmetic (Continued)

COROLLARY 2: Let m be a positive integer and let a and b be integers. Then $(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$ and $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

Proof: By the definitions of mod m and of congruence modulo m, we know that $a \equiv (a \bmod m) (\bmod m)$ and $b \equiv (b \bmod m) (\bmod m)$. Hence, Theorem 5 tells us that $a + b \equiv (a \bmod m) + (b \bmod m) (\bmod m)$ and $ab \equiv (a \bmod m)(b \bmod m) (\bmod m)$.

Example 7: Find the value of $(193 \bmod 31)4 \bmod 23$.

Solution: To compute $(193 \bmod 31)4 \bmod 23$, we will first evaluate $193 \bmod 31$. Because $193 = 6859$ and $6859 = 221 \cdot 31 + 8$, we have $193 \bmod 31 = 6859 \bmod 31 = 8$. So, $(193 \bmod 31)4 \bmod 23 = 84 \bmod 23$. Next, note that $84 = 4096$. Because $4096 = 178 \cdot 23 + 2$, we have $4096 \bmod 23 = 2$. Hence, $(193 \bmod 31)4 \bmod 23 = 2$.

4.1.5 Arithmetic Modulo m

We can define arithmetic operations on $\mathbb{Z}_m$, the set of nonnegative integers less than m, that is, the set $\{0,1,\ldots,m-1\}$. In particular, we define addition of these integers, denoted by $+_m$ by $a +_m b = (a + b) \bmod m$, 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 $a \cdot_m b = (a \cdot b) \bmod m$, where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers. The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo m and when we use these operations, we are said to be doing arithmetic modulo m.

4.1.5 Arithmetic Modulo m (Continued)

Example 8: Use the definition of addition and multiplication in $\mathbb{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definition of addition modulo 11, we find that $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$, and $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$. Hence, $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$.

Properties of closure, associativity, commutativity satisfy, identity elements and additive inverses, distributivity