University of Baghdad
College of Science for Women
Department of Computer Science

Computer Mathematics

Ahmed J. Kadhim, M. Sc.

2023 - 2024

Introduction

In this semester, computer mathematics into four chapter will be studied. The first, known as number theory. In this chapter, some of the important concepts of number theory including many of those used in computer science are developed. In the next chapter, two ways that recurrence relations play important roles in the study of algorithms will be discussed. The Fibonacci recurrence and linear recurrences (linear homogeneous and non-homogeneous recurrences) are studied**.**

In the third chapter, many counting problems in terms of ordered or unordered arrangements of the objects of a set with or without repetitions could be phrased. These arrangements, called permutations and combinations, are used in many counting problems. The last chapter concludes generating functions that can be used to solve many types of counting problems and used to solve recurrence relations by translating a recurrence relation for the terms of a sequence into an equation involving a generating function.

Number Theory

The part of mathematics devoted to the study of the set of integers and their properties is known as number theory. In this chapter we will explain some of the important concepts of number theory including many of those used in computer science.

Division

When one integer is divided by a second nonzero integer, the quotient may or may not be an integer. For example, $12/3 = 4$ is an integer, whereas $11/4 = 2.75$ is not.

Definition: If a and b are integers with $a \neq 0$, we say that a divides b (or b is divisible by a) if there is an integer c such that $b = ac$.

If a divides b, we write $a \mid b$, while if a does not divide b, we write $a \nmid b$.

For example: $-5 \mid 30, 7 \nmid 50, 17 \mid 0$.

Example: The divisor of 6 are $\mp 1, \mp 2, \mp 3$ & ∓ 6, the divisors of 17 are ∓ 1 & ∓ 17.

Example: Determine whether 3 | 7 and whether 3 | 12.

We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$.

Theorem(1): If a, b and c are integers then the following statements hold:

1. $a \mid o, 1 \mid a, a \mid a$.
2. $a \mid \mp 1$ iff $a = \mp 1$.
3. If $a \mid b$ and $c \mid d$ then $ac \mid bd$.
4. If $a \mid b$ and $b \mid c$ then $a \mid c$.
5. $a \mid b$ and $b \mid a$ iff $a = \mp b$.
6. If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.
7. If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for arbitrary integers x and y.
8. Let $a > 0, b > 0$. If $a \mid b$ then $a \leq b$.

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 (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: 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:

$$q = a\,\boldsymbol{div}\,d, \; r = a\,\boldsymbol{mod}\,d.$$

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

We have

$101 = 11 . 9 + 2.$

Hence, the quotient when 101 is divided by 11 is $9 = 101\,\boldsymbol{div}\,11$, and the remainder is $2 = 101\,\boldsymbol{mod}\,11.$

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

We have

$-11 = 3(-4) + 1.$

Hence, the quotient when -11 is divided by 3 is $-4 = -11\,\boldsymbol{div}\,3$, and the remainder is $1 = -11\,\boldsymbol{mod}\,3.$

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 $0 \leq r < 3.$

Modular Arithmetic

Definition: 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 $a \equiv b\ (\boldsymbol{mod}\,m)$. If a and b are not congruent modulo m, we write $a \not\equiv b\ (\boldsymbol{mod}\,m)$.

Theorem: Let a and b be integers, and let m be a positive integer. Then $a \equiv b\ (\boldsymbol{mod}\,m)$ if and only if $a\,\boldsymbol{mod}\,m = b\,\boldsymbol{mod}\,m.$

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

Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5\ (\boldsymbol{mod}\,6)$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14\ (\boldsymbol{mod}\,6)$.

Theorem: Let m be a positive integer. If $a \equiv b\ (\boldsymbol{mod}\,m)$ and $c \equiv d\ (\boldsymbol{mod}\,m)$, then $a + c \equiv b + d\ (\boldsymbol{mod}\,m)$ and $ac \equiv bd\ (\boldsymbol{mod}\,m)$.

<u>Example:</u> Because $7 \equiv 2\ (\boldsymbol{mod}\ 5)\ and\ 11 \equiv 1\ (\boldsymbol{mod}\ 5)$, it follows from previous theorem that

$18 = 7 + 11 \equiv 2 + 1 = 3\ (\boldsymbol{mod}\ 5)$

and that

$77 = 7 \,.\, 11 \equiv 2 \,.\, 1 = 2\ (\boldsymbol{mod}\ 5)$.