Name: Shivani GSI: Madeline Brandt DISC #: 103

Math 55, Handout 7.

SEQUENCES. (156)

1.1. A **sequence** is a discrete structure used to represent an ordered list. A sequence is a function from a subset of the set of ints to a set S

1.2. An **arithmetic progression** is a sequence of the form:

$a, a+d, a+2d, \ldots, a+nd$

where the initial term a and the common difference d are real numbers

1.3. The sum of an arithmetic progression is

$$\sum_{k=0}^{n} a + kd = \frac{n}{2}(2a + (n-1)d)$$

1.4. A **geometric progression** is a sequence of the form:

$a, ar, ar^2, \ldots, ar^n, \ldots$

where the initial term a and the common ratio r are real #s

(164) 1.5. The sum of a geometric progression is

$$\sum_{k=0}^{n} ar^k = \begin{cases} \dfrac{ar^{n+1} - a}{r-1} & \text{if } r \neq 1 \\ (n+1)a & \text{if } r = 1 \end{cases}$$

Q1. Evaluate the sum $\sum_{k=1}^{n}(2k-1)$.

RECURRENCE RELATIONS. ((58)

2.1. A **recurrence relation** for a sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more previous terms of the sequence, namely $a_0, a_1, \ldots, a_{n-1}$, for all integers n with $n \geq n_0$ is a non-negative integer. A sequence is called a solution of a recurrence relation.

Its **initial conditions** are a_0, a_1 ??

Q2. If a sequence satisfies a 3-term recurrence relation, say, $a_n = 3a_{n-1}+4a_{n-2}$, how many initial conditions determine that sequence?

$a_n = 3$

Q3. Write down a closed formula for the nth term of a sequence defined recursively via

$a_0 = 0$ $a_3 = 9$
$a_1 = 3$ $a_4 = 12$
$a_2 = 6$ $a_5 = 15$

$$a_0 = 0, \quad a_1 = 3, \quad a_n = 2a_{n-1} - a_{n-2}.$$

$a_n = 3n$

DIVISION.

3.1. Given $a, b \in \mathbb{Z}$, $a \neq 0$, we say that a **divides** b (and write $a|b$) if there is an integer c such that $b = ac$

3.2. **The division algorithm.** Let $a \in \mathbb{Z}$ and let $d \in \mathbb{N}$. Then there exists $q \in \mathbb{Z}$ (called the) and $r \in \{0, \ldots, d-1\}$ (called the unique ints) such that $a = dq + r$.

In that case, we write

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

ARITHMETIC MODULO m.

4.1. Given $m \in \mathbb{N}$, we can define **arithmetic operations on** $Z_m = \{0, \ldots, m-1\}$ as

$$a +_m b = (a+b) \bmod m$$
$$a \cdot_m b = (a \cdot b) \bmod m$$

4.2. These operations satisfy many properties of ordinary addition and multiplication, e.g.,

Closure - If a and b belong to Z_m, then $a +_m b$ and $a \cdot_m b$ belong to Z_m
Associativity - If a, b, and c belong to Z_m, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$
Commutativity - If a and b belong to Z_m, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$
Identity elements - The elements 0 and 1 are identity elements for addition & multiplication modulo m, respectively.
Additive inverses - If $a \neq 0$ belong to Z_m, then $m-a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is $a +_m (m-a) = 0$ and $0 +_m 0 = 0$
Distributivity - If a, b, and c belong to Z_m, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Q4. Does multiplication modulo m satisfy the property of ordinary multiplication

$$\forall x, y \; [\, x \cdot y = 0 \longrightarrow x = 0 \vee y = 0 \,] \,?$$

$(a \cdot b) \bmod m = 0$ means m must divide $a \cdot b$
if $a = 0$ or $b = 0$, then we get $0 \bmod 5 = 0$ which is a contradiction, as 5×0. Thus, multiplication modulo does not satisfy this ordinary multiplication property

4.3. Let $a, b \in \mathbb{Z}$ and let $m \in \mathbb{N}$. The notation $a \equiv b \pmod{m}$ means that m divides $a - b$

Q5. Suppose $a, b, k, m \in \mathbb{N}$ and $ak \equiv bk \pmod{m}$. Does this imply $a \equiv b \pmod{m}$? Why or why not?

yes it is. $ak \equiv bk \pmod{m}$ implies $ak - bk = lm$ for some $l \in \mathbb{Z}$

If k and m are relatively prime i.e. have no common factors $\mathbb{N} \setminus \{1\}$, then for $k(a-b) = lm$, m must divide $a - b$

therefore, $ak \equiv bk \pmod{m}$ implies $a \equiv b \pmod{m}$ for $a, b, k, m \in \mathbb{N}$