ICSI 210 – Discrete Structures

Instructor: Abram Magner Date: Fall 2022

Instructions: Please answer the following questions in complete sentences, showing all work (including code and output of programs, when applicable). I prefer that you type your solutions (e.g., using LaTeX, with Overleaf, TeXworks, etc., or Word), but will accept handwritten notes. If the grader cannot read your handwriting, then they cannot award you points. **If you do not show your work and just give an answer, then you will get at most 1 point.**

Due date: Tuesday, 11/22/2022, 11:59 p.m.

4.1 Review

1. Evaluate the sum
$$\sum_{j=0}^{5} j. \tag{4.1}$$
Your answer should be a number, with no variables.

2. Consider the odd integers 5 and 11. Find numbers h, k such that $5 = 2h + 1$ and $11 = 2k + 1$.

4.2 Pigeonhole principle

1. Consider a scenario in which 10 pigeons roost in 11 holes. Is it necessarily true that there exists a hole containing two or more pigeons? Justify your answer.

2. Prove the following: in a set of 3 integers, either at least two of them are odd or at least two of them are even.

3. There are 365 days in a year. Consider a set S of 2000 people. For each day $d \in \{1, ..., 365\}$, let n_d denote the number of people in S whose birthday lies on day d. Let d_* denote the day such that n_{d_*} is maximized, over all possible days (i.e., it's the day that is the birthday of the largest number of people in S).

   What is the minimum possible value for d_*? Justify your answer.

4.3 Congruences

1. Let $x \in \mathbb{Z}$. State a modular congruence involving x that is equivalent to x being even. That is, find numbers a and b such that $x \equiv a \mod b$ if and only if x is even.

2. Let $x \in \mathbb{Z}$. Find numbers a and b such that $x \equiv a \mod b$ if and only if x is odd.

4.4 Euclidean algorithm

1. Compute $\gcd(438, 288)$ using the Euclidean algorithm, making sure to show all steps. Find integers a, b such that

$$438a + 288b = \gcd(438, 288). \tag{4.2}$$

4.5 Inverses

1. Does 37 have an inverse modulo 439? If so, compute its inverse.
2. Does 5 have an inverse modulo 6? If so, compute its inverse.

4.1 Review

1. Evaluate the sum

$$\sum_{j=0}^{5} j. \tag{4.1}$$

   Your answer should be a number, with no variables.

2. Consider the odd integers 5 and 11. Find numbers h, k such that $5 = 2h + 1$ and $11 = 2k + 1$.

1. $\sum_{j=0}^{5} j = 0+1+2+3+4+5 = \frac{5(5+1)}{2} = \frac{5 \cdot 6}{2} = 15$

2. $5, 11 \in \mathbb{Z}^+$

Find h s.t. $5 = 2h+1$

$4 = 2h$

$\boxed{h=2}$

Find k s.t. $11 = 2k+1$

$10 = 2k$

$\boxed{k=5}$

4.2 Pigeonhole principle

1. Consider a scenario in which 10 pigeons roost in 11 holes. Is it necessarily true that there exists a hole containing two or more pigeons? Justify your answer.
2. Prove the following: in a set of 3 integers, either at least two of them are odd or at least two of them are even.
3. There are 365 days in a year. Consider a set S of 2000 people. For each day $d \in \{1, ..., 365\}$, let n_d denote the number of people in S whose birthday lies on day d. Let d_* denote the day such that n_{d_*} is maximized, over all possible days (i.e., it's the day that is the birthday of the largest number of people in S).

   What is the minimum possible value for d_*? Justify your answer.

1. Definition: The pigeonhole principle.

If k is a positive integer and $k+1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

Proof. Sine $k=10$, which is the number of pigeons given : there exist $k+1 = 11$ boxes in this scenario.

by pigeonhole principle, there should be $\lceil 10/11 \rceil = 1$ box for each pigeon.

Therefore, a pigeonhole containing two pigeons is possible but not ideal.

2. Prove the following: in a set of 3 integers, either at least two of them are odd or at least two of them are even.

Let $N = 3$, the number of integers in a set.

Let $K = 2$, the catogories of different kind integers either even or odd.

$\lceil \frac{N}{K} \rceil = \lceil \frac{3}{2} \rceil = 2.$

Therefore, we concludes that there will always exist either at least odd integer or at least two even integers.

4.3 Congruences

1. Let $x \in \mathbb{Z}$. State a modular congruence involving x that is equivalent to x being even. That is, find numbers a and b such that $x \equiv a \mod b$ if and only if x is even.
2. Let $x \in \mathbb{Z}$. Find numbers a and b such that $x \equiv a \mod b$ if and only if x is odd.

1. An even number is a number which leaves remainder 0 on divison by 2.

   This indicates that $a=0$ and $b=2$. Thus the congruence is $x \equiv 0 \pmod 2$.

2. An odd number is defined as let $m \in \mathbb{Z}$ s.t. $n = 2m+1$. An odd number remainder 1 on division by 2.

   Thus $a=1$ and $b=2$ and the congruence read as $x \equiv 1 \pmod 2 \Leftrightarrow x$ is odd.

4.4 Euclidean algorithm

1. Compute gcd(438, 288) using the Euclidean algorithm, making sure to show all steps. Find integers a, b such that

$$438a + 288b = \gcd(438, 288). \tag{4.2}$$

Euclidean Algorithm: Input: a, b assume $a > b$.

Output: $\gcd(a, b)$.

1). Compute q, r s.t. $a = qb + r$, $r \in \{0, 1, b-1\}$.

2). Base case: If $r = 0$, then output b.

3). Recursion: Otherwise, set $a := b$, $b := r$, and go back to step

a	b	q	r
438	288	1	150
288	150	1	138
150	138	1	12
138	12	11	6
12	$\boxed{6}$	2	0

$\therefore \gcd(438, 288) = 6$.

Find $438a + 288b = 6$.

Let $6 = 1(138) - 11(12)$

$6 = 1(138) - 11(150 - 138)$

$6 = -11(150) + 12(138)$

$6 = -11(150) + 12(288 - 150)$

$6 = -23(150) + 12(288)$

$6 = -23(438 - 288) + 12(288)$

$6 = 35(288) - 23(438)$.

$\therefore \boxed{a = -23}$; $\boxed{b = 35}$

4.5 Inverses

1. Does 37 have an inverse modulo 439? If so, compute its inverse.
2. Does 5 have an inverse modulo 6? If so, compute its inverse.

Definition: We say that integers a and b are multiplicative inverses modulo m if $ab \equiv 1 \pmod{m}$.

Theorem: The integer a has an inverse modulo m if and only if $\gcd(a, m) = 1$.

if $\gcd(a, m) > 1$, then it modular inverse DNE.

1. $37 \cdot x \equiv 1 \bmod 439$

$1 \equiv 440 \equiv 879 \equiv 1318 \equiv 1757 \equiv 2196 \equiv 2635 \equiv 3074 \equiv 3513 \equiv 3952 \equiv 4391 \equiv 4830 \equiv 5269$

$\equiv 5708 \equiv 6147 \equiv 6586 \pmod{1}$

37 178

$\boxed{37^{-1} \equiv 178 \pmod{439}}$

2. $5 \cdot x \equiv 1 \bmod 6$

$\boxed{5^{-1} \equiv 5 \pmod{6}}$