MAT 258–Discrete Mathematics

Fall 2018

Prerequisites: MAT 200 or MAT 230

General Information

Class Schedule: Wednesdays and Fridays 5:00–6:20pm
Classroom: Lecture Theater 5B
Instructor: Michael Daniel Samson
Contact: `mat258@mdvsamson.work`, +65 6577 1944
Class Webpage: Moodle, `mdvsamson.work/mat258`
Office Hours: Wednesdays and Fridays 6:30–7:30pm, Mondays 2:00–7:00pm or by appointment (through email)

Description

This course gives an introduction to several mathematical topics of foundational importance in the mathematical and computer sciences. Typically starting with propositional and first-order logic, the course considers applications to methods of mathematical proof and reasoning. Further topics include basic set theory, number theory, enumeration, recurrence relations, mathematical induction, generating functions, and basic probability. Other topics may include graph theory, asymptotic analysis, and finite automata.

Course Objectives and Learning Outcomes

Upon completing this course students should be able to:

- Apply congruence classes to computational problems.
- Analyze logical statements and determine their truth tables.
- Formulate the steps of a valid mathematical proof.
- Construct inductive schemes and recursive functions for computational applications.
- Understand and apply combinatorial expressions for enumeration problems.
- Apply advanced counting techniques when required.
- Understand and compute discrete probabilities.

Textbooks

Discrete Mathematics and Its Applications, 7th edition, Global Edition, Kenneth Rosen, Kamala Krithivasan, McGraw-Hill, ISBN-13 978-0-07-131501-2

Outline and Tentative Dates

The following schedule is subject to change.

Sets and Numbers
September 5: Sets
September 7: Set Operations
September 12: Functions
September 14: Cardinality
September 19, 21: Modular Arithmetic, Congruences
September 26: **Quiz**, Representations
September 28: Closures
October 3, 5: Equivalences, Partial Orders
October 10: **Examination** (discussion on October 12)
Logic and Proofs
October 17, 19: Propositional Logic, Proofs
October 24, 26: **Quiz**, Mathematical Induction
October 31, November 2: Recursive Definitions
November 6: *Deepavali*
November 7: **Examination** (discussion on November 9)
Counting and Probability
November 14: Permutations and Combinations
November 16: Binomial Coefficients
November 21, 23: Generating Functions
November 28: Inclusion-Exclusion, **Quiz**
November 30, December 5: Bayes's Theorem
December 7: Expected Value and Variance
December 10–14: **Examination** (schedule to be announced by DigiPen Admin)

Grading Policy

The examination on week fifteen is *optional*. You must inform the instructor of your decision to not take the final exam *by week fourteen*.

The relative weights of homework and examinations are:

10% Homework (given during non-examination weeks)
30% Quizzes (drop the lowest)
60% Examinations (drop the lowest)

Grades will be computed out of 40 points. Letter grades will be computed subject to:

35 = at least A
30 = at least B
20 = at least C- (passing)

To pass the course, you need to

***have a passing examination average** and **the course total should be greater than or equal to 20**.*

Late Policy

Late assignments **will not** be accepted. There will be **no make-up** exams, unless authorized by the instructor.

Last Day to Withdraw

The final date to withdraw from this course is **28 October 2018**. Scores for six (6) homework submissions, two (2) quizzes and one (1) examination should be available before this date. In order to withdraw from a course, in accordance with policy, contact your advisor or the Registrar to begin the withdrawal process—it is *not sufficient* simply to stop attending class or to inform the instructor. The last day for withdrawal from this course is cited in the official catalog.

Academic Integrity Policy

Academic dishonesty *in any form* will not be tolerated in this course. Cheating, copying, plagiarizing, or any other form of academic dishonesty (including doing someone else's individual assignments) will result in, at the very minimum, a zero on the assignment in question, and could result in a failing grade in the course or even expulsion from DigiPen.

External Preparation

It is expected that the students in this class spend six (6) hours on average per week for outside classroom activities through the semester, including, but not limited to, homework, reading assignments, project implementation, group discussions, preparation of examinations, etc.

Disability Support Service

Students who have special needs or medical conditions and require formal accommodations in order to fully participate or effectively demonstrate learning in this class should contact the Student Life & Advising Office (`studentlife.sg@digipen.edu`) at the beginning of each semester. A Student Life & Advising Officer will meet with the student privately to discuss how the accommodations will be implemented.

Name: _____

§2.1 #7 For each of the following sets, determine whether $\{2\}$ is an element of that set.

(a) $\{x \in \mathbb{R} \mid x \text{ is an integer greater than } 1\}$
Since the elements of this set are real numbers, the set $\{2\}$ is not an element of this set.

(b) $\{x \in \mathbb{R} \mid x \text{ is the square of an integer}\}$
Since the elements of this set are real numbers, the set $\{2\}$ is not an element of this set.

(c) $\{2, \{2\}\}$
Yes, the elements of this set are the number 2 and the set $\{2\}$.

(d) $\{\{2\}, \{\{2\}\}\}$
Yes, the elements of this set are the sets $\{2\}$ and $\{\{2\}\}$, the set containing only the set $\{2\}$.

(e) $\{\{2\}, \{2, \{2\}\}\}$
Yes, the elements of this set are the sets $\{2\}$ and $\{2, \{2\}\}$, the set in (c).

(f) $\{\{\{2\}\}\}$
The only element of this set is the set $\{\{2\}\}$, the set containing only the set $\{2\}$, so the set $\{2\}$ is not an element of this set.

§2.1 #15 Find the power set of each of these sets, where a and b are distinct elements

(a) $\{a\}$
$\mathscr{P}(\{a\}) = \{\varnothing, \{a\}\}$.

(b) $\{a, b\}$
$\mathscr{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$.

(c) $\{\varnothing, \{\varnothing\}\}$
$\mathscr{P}(\{\varnothing, \{\varnothing\}\}) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$.

§2.1 #29 This exercise presents *Russell's paradox*. Let S be the set that contains a set x if the set x does not belong to itself, so that $S = \{x \mid x \notin x\}$.

(a) Show the assumption that S is a member of S leads to a contradiction.
If $S \in S$, by the definition of S, $S \notin S$, which is contradicts the assumption.

(b) Show the assumption that S is not a member of S leads to a contradiction.
If $S \notin S$, by the definition of S, $S \in S$, which is contradicts the assumption.

By parts (a) and (b), it follows that the set S cannot be defined as it was. This paradox can be avoided by restricting the types of elements that sets can have.

§2.2 #23 The *symmetric difference* of A and B, denoted by $A \oplus B$, is the set containing those elements in either A or B, but not in both A and B. Suppose that A, B, and C are sets such that $A \oplus C = B \oplus C$. Must it be the case that $A = B$?

First, note that $A \oplus C = (A \cup C) - (A \cap C) = (A \cap C^{\mathrm{c}}) \cup (A^{\mathrm{c}} \cap C)$, a disjoint union. Since those sets are equal, $(A \oplus C) \cap C^{\mathrm{c}} = (B \oplus C) \cap C^{\mathrm{c}}$, which gives $A \cap C^{\mathrm{c}} = B \cap C^{\mathrm{c}}$; also, $(A \oplus C) \cap C = (B \oplus C) \cap C$ gives $A^{\mathrm{c}} \cap C = B^{\mathrm{c}} \cap C$, whose complements are also equal: by De Morgan's Laws, $A \cup C^{\mathrm{c}} = B \cup C^{\mathrm{c}}$. For these last two sets, $(A \cup C^{\mathrm{c}}) \cap C = (B \cup C^{\mathrm{c}}) \cap C$, which gives $A \cap C = B \cap C$—this, with the first equality derived above, by union, gives $(A \cap C) \cup (A \cap C^{\mathrm{c}}) = (B \cap C) \cup (B \cap C^{\mathrm{c}})$, which gives $A = B$.

§2.2 #31 Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ if, for every positive integer i,

(a) $A_i = \{-i, -i+1, \ldots, -1, 0, 1, \ldots, i-1, i\}$
0 is in all sets A_i, $n > 0$ is in the set A_n, and $n < 0$ is in the set A_{-n}, so all integers are in $\bigcup_{i=1}^{\infty} A_i$ and $\mathbb{Z} \subseteq \bigcup_{i=1}^{\infty} A_i$. For all A_i, $A_i \subset \mathbb{Z}$, so $\bigcup_{i=1}^{\infty} A_i \subseteq \mathbb{Z}$, and $\bigcup_{i=1}^{\infty} A_i = \mathbb{Z}$.

$A_1 \subset A_i$ for all A_i, so $A_1 \subseteq \bigcap_{i=1}^{\infty} A_i$. For $n > 1$, $n \notin A_{n-1}$, and $n < -1$, $n \notin A_{-n-1}$ and $A_i \subset \mathbb{Z}$, so $\bigcap_{i=1}^{\infty} A_i$ doesn't include integers n, $|n| > 1$, so $\bigcap_{i=1}^{\infty} A_i = A_1$.

(b) $A_i = \{-i, i\}$

0 is in none of the sets A_i, $n > 0$ is in the set A_n, and $n < 0$ is in the set A_{-n}, so all nonzero integers are in $\bigcup_{i=1}^{\infty} A_i$ and $(\mathbb{Z} - \{0\}) \subseteq \bigcup_{i=1}^{\infty} A_i$. For all A_i, $A_i \subset \mathbb{Z}$, so $\bigcup_{i=1}^{\infty} A_i \subseteq (\mathbb{Z} - \{0\})$, and $\bigcup_{i=1}^{\infty} A_i = (\mathbb{Z} - \{0\})$.

Since $A_1 \cap A_2 = \varnothing$, and $\bigcap_{i=1}^{\infty} A_i \subseteq A_1 \cap A_2$, then $\bigcap_{i=1}^{\infty} A_i = \varnothing$.

(c) $A_i = [-i, i]$, that is, the set of real numbers x with $-i \leq x \leq i$

The sets telescope: since $A_i \subset A_{i+1}$, $A_i \cup A_{i+1} = A_{i+1}$ and $A_i \cap A_{i+1} = A_i$, and $\bigcap_{i=1}^{\infty} A_i = A_1 = [-1, 1]$.

For $x \geq 0$, $n = \lceil x \rceil \geq x$ and $x \in A_n$; for $x < 0$, $n = \lfloor x \rfloor \leq x$ and $x \in A_n$, so $\mathbb{R} \subseteq \bigcup_{i=1}^{\infty} A_i$. For all A_i, $A_i \subset \mathbb{R}$, so $\bigcup_{i=1}^{\infty} A_i \subseteq \mathbb{R}$, and $\bigcup_{i=1}^{\infty} A_i = \mathbb{R}$.

(d) $A_i = [i, \infty)$, that is, the set of real numbers x with $x \geq i$

The sets telescope: since $A_{i+1} \subset A_i$, $A_i \cup A_{i+1} = A_i$ and $A_i \cap A_{i+1} = A_{i+1}$, and $\bigcup_{i=1}^{\infty} A_i = A_1 = [1, \infty)$.

For $x \geq 1$, $n = \lfloor x \rfloor + 1 > x$ and $x \notin A_n$, so $x \notin \bigcap_{i=1}^{\infty} A_i$. Therefore $\bigcap_{i=1}^{\infty} A_i = \varnothing$.

Name: _____

§2.3 #19 Suppose that g is a function from A to B and f is a function from B to C.

(a) Show that if both f and g are one-to-one functions, then $f \circ g$ is also one-to-one.
Consider that, for $a, b \in A$, $f(g(a)) = f(g(b))$. Since f is one-to-one, then $g(a) = g(b)$; since g is one-to-one, $a = b$. Thus, $(f \circ g)(a) = (f \circ g)(b)$ means $a = b$, $f \circ g$ is one-to-one.

(b) Show that if both f and g are onto functions, then $f \circ g$ is also onto.
Consider $c \in C$: since f is onto, there exists $b \in B$ such that $f(b) = c$; since g is onto, there exists $a \in A$ such that $g(a) = b$. Thus, $f(g(a)) = c$, and, since for any $c \in C$, there exists $a \in A$ such that $(f \circ g)(a) = c$, $f \circ g$ is onto.

§2.3 #47 Let S be a subset of a universal set U. The *characteristic function* f_S of S is the function from U to the set $\{0, 1\}$ such that $f_S(x) = 1$ if x belongs to S and $f_S(x) = 0$ if x does not belong to S. Let A and B be sets. Show that for all $x \in U$,

(a) $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$
If $x \notin A$ and $x \notin B$, then $x \notin A \cap B$ so $f_A(x) = 0$, $f_B(x) = 0$ and $f_{A \cap B}(x) = 0$, so $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$.
If $x \in A$ and $x \notin B$, then $x \notin A \cap B$ so $f_A(x) = 1$, $f_B(x) = 0$ and $f_{A \cap B}(x) = 0$, so $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$.
If $x \notin A$ and $x \in B$, then $x \notin A \cap B$ so $f_A(x) = 0$, $f_B(x) = 1$ and $f_{A \cap B}(x) = 0$, so $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$.
If $x \in A$ and $x \in B$, then $x \in A \cap B$ so $f_A(x) = 1$, $f_B(x) = 1$ and $f_{A \cap B}(x) = 1$, so $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$.

(b) $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$
If $x \notin A$ and $x \notin B$, then $x \notin A \cup B$ so $f_A(x) = 0$, $f_B(x) = 0$ and $f_{A \cup B}(x) = 0$, so $f_{A \cap B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$.
If $x \in A$ and $x \notin B$, then $x \in A \cup B$ so $f_A(x) = 1$, $f_B(x) = 0$ and $f_{A \cup B}(x) = 1$, so $f_{A \cap B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$.
If $x \notin A$ and $x \in B$, then $x \in A \cup B$ so $f_A(x) = 0$, $f_B(x) = 1$ and $f_{A \cup B}(x) = 1$, so $f_{A \cap B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$.
If $x \in A$ and $x \in B$, then $x \in A \cup B$ so $f_A(x) = 1$, $f_B(x) = 1$ and $f_{A \cup B}(x) = 1$, so $f_{A \cap B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$.

(c) $f_{\bar{A}}(x) = 1 - f_A(x)$
If $x \notin A$, then $x \in \bar{A} = U - A$ so $f_A(x) = 0$ and $f_{\bar{A}}(x) = 1$, so $f_{\bar{A}}(x) = 1 - f_A(x)$.
If $x \in A$, then $x \notin \bar{A}$ so $f_A(x) = 1$ and $f_{\bar{A}}(x) = 0$, so $f_{\bar{A}}(x) = 1 - f_A(x)$.

(d) $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x) \cdot f_B(x)$, where $A \oplus B$ is the *symmetric difference* of A and B, is the set containing those elements in either A or B, but not in both A and B.
If $x \notin A$ and $x \notin B$, then $x \notin A \oplus B$ so $f_A(x) = 0$, $f_B(x) = 0$ and $f_{A \oplus B}(x) = 0$, so $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x) \cdot f_B(x)$.
If $x \in A$ and $x \notin B$, then $x \in A \oplus B$ so $f_A(x) = 1$, $f_B(x) = 0$ and $f_{A \oplus B}(x) = 1$, so $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x) \cdot f_B(x)$.
If $x \notin A$ and $x \in B$, then $x \in A \oplus B$ so $f_A(x) = 0$, $f_B(x) = 1$ and $f_{A \oplus B}(x) = 1$, so $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x) \cdot f_B(x)$.
If $x \in A$ and $x \in B$, then $x \notin A \oplus B$ so $f_A(x) = 1$, $f_B(x) = 1$ and $f_{A \oplus B}(x) = 0$, so $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x) \cdot f_B(x)$.

§2.3 #48 Suppose that f is a function from A to B, where A and B are finite sets with $|A| = |B|$. Show that f is one-to-one if and only if it is onto.

If $A = B = \varnothing$, and $f : A \to B$ is vacuously one-to-one and onto, since f cannot define any mapping over nonexistent elements. Let $|A| = |B| = n \in \mathbb{N}$, such that $f(a_i) = b_i$, for $i = 1, \ldots, n$, for $a_i \in A$ and $b_i = B$. If there exist $b_i = b_j$, $1 \leq i < j \leq n$, then f is not one-to-one: that also means that $|f(A)| < n$, since two images coincide, so $f(A) \subset B$ and $f(A) \neq B$, and f is not onto.

If, on the other hand, f is one-to-one, then $|f(A)| = |A| = |B|$—since $f(A) \subseteq B$ and B is finite, this is only true if $f(A) = B$, and f is onto. Since if f is not one-to-one, it is not onto, and if f is one-to-one, it is also onto, it follows that if f is onto, then it is one-to-one, and the proof concludes.

§2.5 #1 Determine whether each of these sets is finite, countably infinite, or uncountable. For those that are countably infinite, exhibit a one-to-one correspondence (bijection) between the set of positive integers and that set.

(a) the negative integers
$\mathbb{Z}^-$ is countably infinite, with bijection $f : \mathbb{Z}^+ \to \mathbb{Z}^-$, $f(n) = -n$.

(b) the even integers
$2\mathbb{Z}$ is countably infinite, with bijection $f : \mathbb{Z}^+ \to 2\mathbb{Z}$, $f(n) = \begin{cases} n-1, & \text{if } n \bmod 2 = 1, \\ -n, & \text{if } n \bmod 2 = 0. \end{cases}$

(c) the integers less than 100
$S = \{n \in \mathbb{Z}, n < 100\}$ is countably infinite, with bijection $f : \mathbb{Z}^+ \to S$, $f(n) = 100 - n$.

(d) the real numbers between 0 and $\frac{1}{2}$
$\left(0, \frac{1}{2}\right)$ is uncountable, $f : (0,1) \to \left(0, \frac{1}{2}\right)$, $f(x) = \frac{x}{2}$ is a bijection and $(0,1)$ is uncountable.

(e) the positive integers less than 1000000000
$|\{n \in \mathbb{Z}^+, n < 1000000000\}| = 999999999$, and the set is finite

(f) the integers that are multiples of 7
$7\mathbb{Z}$ is countably infinite, with bijection $f : \mathbb{Z}^+ \to 7\mathbb{Z}$, $f(n) = \begin{cases} \frac{7(n-1)}{2}, & \text{if } n \bmod 2 = 1, \\ -\frac{7n}{2}, & \text{if } n \bmod 2 = 0. \end{cases}$

§2.5 #18 Show that there is no infinite set A such that $|A| < |\mathbb{Z}^+| = \aleph_0$.

Given an onto function $f : \mathbb{Z}^+ \to A$ (a complete enumeration of A), implying $|A| \leq |\mathbb{Z}^+|$—thus, for every $a \in A$, there is at least one pre-image $n \in \mathbb{Z}^+$, such that $f(n) = a$. Consider the function $g : A \to \mathbb{Z}^+$, where $g(a) = \min\{n \mid f(n) = a\}$ (a partial inversion of f), and $h : g(A) \to \mathbb{Z}^+$, where $h(n) = i$ if n is the ith smallest element of $g(A)$ (ordering the images of $g(A)$ in ascending order).

g and h are one-to-one, so $h \circ g : A \to \mathbb{Z}^+$ is one-to-one. There are only two possibilities for $h \circ g$:

- $h \circ g$ is onto: then $h \circ g$ is a bijection between A and $\mathbb{Z}^+$, and $|A| = |\mathbb{Z}^+| = \aleph_0$
- $h \circ g$ is not onto: then there are a finite number of elements of $g(A)$, and $h(g(A))$ has a maximum element $N \in \mathbb{Z}^+$, so $|A| = N$, and A is a finite set.

Thus, a contradiction occurs: either A is finite (not infinite), or A is countably infinite.

Source: Kenneth Rosen and Kamala Krithivasan, *Discrete Mathematics and Its Applications*, 7th ed

Name: _____

§4.3 #14 We call a positive integer *perfect* if it equals the sum of its positive divisors other than itself.

(a) Show that 6 and 28 are perfect.
The factors of $6 = 2^{2-1}(2^2-1)$ are 1, 2, 3 and 6, and $1+2+3=6$. The factors of $28 = 2^{3-1}(2^3-1)$ are 1, 2, 4, 7, 14 and 28, and $1+2+4+7+14=28$.

(b) Show that $2^{p-1}(2^p-1)$ is a perfect number when 2^p-1 is prime.
The factors of $2^{p-1}(2^p-1)$ are $1, 2, \ldots, 2^{p-1}, 2^p-1, 2(2^p-1), \ldots, 2^{p-2}(2^p-1)$ and $2^{p-1}(2^p-1)$, and

$$\begin{aligned}1+2+\cdots+2^{p-1}+(2^p-1)+2(2^p-1)+\cdots+2^{p-2}(2^p-1) &= \sum_{k=0}^{p-1} 2^k + (2^p-1)\sum_{\ell=0}^{p-2} 2^\ell \\ &= (2^p-1)+(2^p-1)(2^{p-1}-1) \\ &= 2^{p-1}(2^p-1).\end{aligned}$$

§4.3 #29 Using the coefficients in the Euclidean method for determining the greatest common divisor, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

(a) 10, 11
Since $11 = 10+1$ and $\gcd(11,10)=1$, $\gcd(11,10) = 11-10$.

(b) 21, 44
Since $44 = 2(21)+2$, $21 = 2(10)+1$ and $\gcd(44,21)=1$, $\gcd(44,21) = 21-2(10) = 21-10[44-2(21)] = 21(21)-10(44)$.

(c) 36, 48
Since $48 = 36+12$ and $\gcd(48,36)=12$, $\gcd(48,36) = 48-36$.

(d) 34, 55
Since $55 = 34+21$, $34 = 21+13$, $21 = 13+8$, $13 = 8+5$, $8 = 5+3$, $5 = 3+2$, $3 = 2+1$ and $\gcd(55,34)=1$,

$$\begin{aligned}\gcd(55,34) &= 3-2 = 3-(5-3) = 2(8-5)-5 = 2(8)-3(13-8) = 5(21-13)-3(13) \\ &= 5(21)-8(34-21) = 13(55-34)-8(34) = 13(55)-21(34).\end{aligned}$$

Notice the terms of the Fibonacci sequence appearing in both directions.

(e) 117, 213
Since $213 = 117+96$, $117 = 96+21$, $96 = 4(21)+12$, $21 = 12+9$, $12 = 9+3$ and $\gcd(213,117)=3$,

$$\begin{aligned}\gcd(213,117) &= 12-9 = 12-(21-12) = 2[96-4(21)]-21 = 2(96)-9(117-96) \\ &= 11(213-117)-9(117) = 11(213)-20(117).\end{aligned}$$

(f) 0, 223
Since $\gcd(0,223)=223$, $\gcd(0,223) = 0+223$.

(g) 123, 2347
Since $2347 = 19(123)+10$, $123 = 12(10)+3$, $10 = 3(3)+1$ and $\gcd(2347,123)=1$,

$$\begin{aligned}\gcd(2347,123) &= 10-3(3) = 10-3[123-12(10)] = 37[2347-19(123)]-3(123) \\ &= 37(2347)-706(123).\end{aligned}$$

(h) 3454, 4666
Since $4666 = 3454+1212$, $3454 = 2(1212)+1030$, $1212 = 1030+182$, $1030 = 5(182)+120$, $182 = 120+62$, $120 = 62+58$, $62 = 58+4$, $58 = 14(4)+2$ and $\gcd(4666,3454)=2$,

$$\begin{aligned}\gcd(4666,3454) &= 58-14(4) = 58-14(62-58) = 15(120-62)-14(62) \\ &= 15(120)-29(182-120) = 44[1030-5(182)]-29(182) \\ &= 44(1030)-249(1212-1030) = 293[3454-2(1212)]-249(1212) \\ &= 293(3454)-835(4666-3454) = 1128(3454)-835(4666).\end{aligned}$$

(i) 9999, 11111

Since $11111 = 9999 + 1112$, $9999 = 8(1112) + 1103$, $1112 = 1103 + 9$, $1103 = 122(9) + 5$, $9 = 5 + 4$, $5 = 4 + 1$ and $\gcd(11111, 9999) = 1$,

$$\begin{aligned}\gcd(11111, 9999) = 5 - 4 = 5 - (9 - 5) &= 2[1103 - 122(9)] - 9 = 2(1103) - 245(1112 - 1103)\\ &= 247[9999 - 8(1112)] - 245(1112) = 247(9999) - 2221(11111 - 9999)\\ &= 2468(9999) - 2221(11111).\end{aligned}$$

§4.4 #13 This exercise outlines a proof of Fermat's little theorem.

(a) Suppose that a is not divisible by the prime p. Show that no two of the integers $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ are congruent modulo p.

If that is not true, then there exist $1 \leq m < n < p$ such that $ma \equiv na \pmod{p}$, so $p \mid (n-m)a$. From the statement below, since p is prime, $p \mid a$ (which contradicts the given) or $p \mid m-n$—this cannot be true, since $1 \leq n - m < p$. Thus, the statement is true.

(b) Conclude from part (a) that the product of $1, 2, \ldots, p-1$ is congruent modulo p to the product of $a, 2a, \ldots, (p-1)a$. Use this to show that $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$.

Since no two of the integers $1 \cdot a$, $2 \cdot a$, $\ldots$, $(p-1) \cdot a$ are congruent modulo p, and, for $1 \leq n < p$, $na \not\equiv 0 \pmod{p}$ (otherwise p divides na, so, from below, p divides n, which is a contradiction), $na \equiv m \pmod{p}$, for $1 \leq m < p$. From this, $\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$ must be a rearrangement of $\{1, 2, \ldots, p-1\}$, so

$$a \cdot 2a \cdot \cdots \cdot (p-1)a = a^{p-1}(p-1)! \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) = (p-1)! \pmod{p}.$$

(c) Show from part (b) that $a^{p-1} \equiv 1 \pmod{p}$ if $p \not| a$.

Hint: Use

> If p is prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

to show that p does not divide $(p-1)!$, then use

> Let m be a positive integer and let a, b and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

If p divides $(p-1)!$, the first statement would indicate that p divides some n, $1 \leq n < p$ which is a contradiction, so p does not divide $(p-1)!$ and, since p is prime, $\gcd(p, (p-1)!) = 1$, thus, by the second statement, $a^{p-1} \equiv 1 \pmod{p}$.

(d) Use part (c) to show that $a^p \equiv a \pmod{p}$ for all integers a.

From above, if p does not divide a, $a^{p-1} \equiv 1 \pmod{p}$, so multiplying both sides of the congruence by a gives $a^p \equiv a \pmod{p}$. If p does divide a, then $a \equiv 0 \pmod{p}$ and $a^p \equiv 0 \equiv a \pmod{p}$.

§4.4 #26 (a) Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

Since 5, 7, 11, 13 are prime, they are pairwise relatively prime, so by Fermat's little theorem, $5^{p-1} \equiv 1 \pmod{p}$, $p = 7, 11, 13$. Thus:

$$\begin{aligned}2003 \equiv 5 \pmod{6} &\implies 5^{2003} = 5^{6a+5} = (5^6)^a 5^5 \equiv 1^a \cdot 5^5 = 5 \cdot 625 \equiv 5 \cdot 2 \equiv 3 \pmod{7};\\ 2003 \equiv 3 \pmod{10} &\implies 5^{2003} = 5^{10b+3} = (5^{10})^b 5^3 \equiv 1^b \cdot 5^3 = 5 \cdot 25 \equiv 5 \cdot 3 \equiv 4 \pmod{11};\\ 2003 \equiv 11 \pmod{12} &\implies 5^{2003} = 5^{12c+11} = (5^{12})^c 5^{11} \equiv 1^c \cdot 5^1 1 = 5 \cdot 25 \cdot (625)^2 \equiv 8 \pmod{13}.\end{aligned}$$

(b) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Letting $M = 1001$ gives us the following set-up for the Chinese remainder theorem:

$$\begin{aligned}m_1 = 7 &\implies M_1 = 143 \equiv 3 \pmod{m_1} &&\implies 3 \cdot 5 = 15 \equiv 1 \pmod{m_1} &&\implies a_1 = 5;\\ m_2 = 11 &\implies M_2 = 91 \equiv 3 \pmod{m_2} &&\implies 3 \cdot 4 = 12 \equiv 1 \pmod{m_2} &&\implies a_2 = 4;\\ m_1 = 13 &\implies M_3 = 77 \equiv 12 \pmod{m_3} &&\implies 12 \cdot 12 = 144 \equiv 1 \pmod{m_3} &&\implies a_3 = 12.\end{aligned}$$

Thus,

$$5^{2003} \equiv \sum_{i=1}^{3} n_i a_i M_i = 3 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12 = 2145 + 1456 + 7392 \pmod{1001}$$
$$\equiv 143 + 455 + 385 = 983 \pmod{1001}.$$

§4.6 #15 What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671? (First, express your answers without computing modular exponentiations. Then use a computational aid to complete these computations. To decrypt, first find the decryption exponent d which is the inverse of $e = 13$ modulo $42 \cdot 58$.)

Noting $42 \cdot 58 = 2436$, by Euclid's algorithm, the Bézout coefficients can be determined: $1 = 937 \cdot 13 - 5 \cdot 2436$, so $937 \cdot 13 \equiv 1 \pmod{2436}$ and $d = 937$. Thus, the original message would be $667^{937} \mod 2537 = 1808$, $1947^{937} \mod 2537 = 1121$, $671^{937} \mod 2537 = 0417$—SILVER.

Name: _____

§9.1 #4 Determine whether the relation R on the set of all integers is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in R$ if and only if

(a) $x \neq y$

Since it is not true that $x \neq x$, it is not reflexive. Since $x \neq y$ implies $y \neq x$, it is symmetric, and not antisymmetric. Since $x \neq y$ and $y \neq x$ do not imply that $x \neq x$, it is not transitive.

(b) $xy \geq 1$

Since it is not true that $x^2 \geq 1$ when $x = 0 \in \mathbb{Z}$, it is not reflexive. Since $xy \geq 1$ implies $yx \geq 1$, even when $x \neq y$, it is symmetric, and not antisymmetric. Since $xy \geq 1$ and $yz \geq 1$ imply that $xy^2z > 0$ and $x, y, z \neq 0$, so $xz > 0$—if the product of two integers is positive, it must be a positive integer, i.e. $xz \geq 1$, so it is transitive.

(c) $x = y + 1$ or $x = y - 1$

Since it is not true that $x = x \pm 1$, it is not reflexive. Since $x = y \pm 1$ implies $y = x \mp 1$, it is symmetric, and not antisymmetric. Since $x = y \pm 1$ and $y = z \pm 1$, either $x = z$ or $x = z \pm 2$, it is not transitive.

(d) $x \equiv y \pmod 7$

Since $x \equiv x \pmod 7$, it is reflexive. Since $x \equiv y \pmod 7$ implies $x - y = 7k$, $k \in \mathbb{Z}$, $y - x = 7(-k)$, and $y \equiv x \pmod 7$, even when $x \neq y$, it is symmetric, and not antisymmetric. Since $x \equiv y \pmod 7$ and $y \equiv z \pmod 7$ imply that $x - y = 7m$ and $y - z = 7n$, $m, n \in \mathbb{Z}$, so $x - z = 7(m + n)$ and $x \equiv z \pmod 7$, so it is transitive.

(e) x is a multiple of y

Since $x \mid x$, it is reflexive. Since $y \mid x$ implies $x = ky$, $k \in \mathbb{Z}$, then $y = \dfrac{x}{k}$, and $\dfrac{1}{k} \notin \mathbb{Z}$, if $k \neq \pm 1$, it is not symmetric, and is not antisymmetric (as $-k \mid k$ and $k \mid -k$). Since $y \mid x$ and $z \mid y$, then $x = my$, $y = nz$ where $m, n \in \mathbb{Z}$, $x = (mn)z$, so $z \mid x$ and it is transitive.

(f) x and y are both negative or both nonnegative

If $x \in \mathbb{Z}^-$, then x and x are both negative; if $x \in \mathbb{W}$, then x and x are both nonnegative—thus, it is reflexive. If x and y are both negative, then y and x are both negative; if x and y are both nonnegative, then y and x are both nonnegative—since these are true even when $x \neq y$, it is symmetric, and not antisymmetric. If (x, y) and (y, z) are in the relation, then consider y: if $y \in \mathbb{Z}^-$, then x and y are both negative, and y and z are both negative, so both x and z are negative, and (x, z) is in the relation; if $y \in \mathbb{W}$, then x and y are both nonnegative, and y and z are both nonnegative, so x and z are both nonnegative, so (x, z) is in the relation—thus, it is transitive.

(g) $x = y^2$

Since $x = x^2$ only if $x = 0$ or $x = 1$, it is not reflexive. Since $x = y^2$ implies $y = \pm\sqrt{x}$, it is not symmetric, and is antisymmetric. Since $x = y^2$ and $y = z^2$ imply that $x = z^4$, it is not transitive.

(h) $x \geq y^2$

Since $x \geq x^2$ only if $x = 0$ or $x = 1$, it is not reflexive. Since $x \geq y^2$ implies $y \leq \pm\sqrt{x}$, it is not symmetric, and is antisymmetric. Since $x \geq y^2$ and $y \geq z^2$ imply that $x \geq z^4 \geq z^2$, since $z^2 \geq 0$, and $f(x) = x^2$ is an increasing function, it is transitive.

§9.1 #17 Let R be a relation from a set A to a set B. The *inverse relation* from B to A, denoted by R^{-1}, is the set of ordered pairs $\{(b, a) \mid (a, b) \in R\}$. The *complementary relation* $\bar{R}$ is the set of ordered pairs $\{(a, b) \mid (a, b) \notin R\}$.

Let R be the relation $R = \{(a, b) \mid a \text{ divides } b\}$ on the set of positive integers. Find (a) R^{-1} and (b) $\bar{R}$.

$R^{-1} = \{(a, b) \mid b \text{ divides } a\}$; $\bar{R} = \{(a, b) \mid a \text{ does not divide } b\}$.

§9.1 #21 Let A be the set of students at your school and B the set of book in the school library. Let R_1 and R_2 be the relations consisting of all ordered pairs (a, b), where student a is required to read book b in a course, and where student a has read book b, respectively. Describe the ordered pairs in each of these relations.

(a) $R_1 \cup R_2$
$(a, b) \in R_1 \cup R_2$ if student a is either required to read or has already read book b.

(b) $R_1 \cap R_2$
$(a, b) \in R_1 \cap R_2$ if student a is either required to read and has already read book b.

(c) $R_1 \oplus R_2$
$(a, b) \in R_1 \oplus R_2$ if student a is either required to read and has not already read book b or student a is not required to read and has already read book b.

(d) $R_1 - R_2$
$(a, b) \in R_1 - R_2$ if student a is required to read and has not already read book b.

(e) $R_2 - R_1$
$(a, b) \in R_2 - R_1$ if student a is not required to read and has already read book b.

§9.1 #41 Let R be a relation that is reflexive and transitive. Prove that $R^n = R$ for all positive integers n.

If $R^2 = R$, then $R^3 = R^2 \circ R = R \circ R = R^2 = R$, and $R^n = R$ for all positive integers n, so it suffices to show that $R^2 = R$ if R is reflexive and transitive. Since R is transitive, if $(a, b), (b, c) \in R$, $(a, c) \in R$, by definition $(a, c) \in R^2$, so $R^2 \subseteq R$. Since R is reflexive, if $(a, b) \in R$, $(a, a) \in R$, and $(a, b) \in R^2$, so $R \subseteq R^2$: thus $R^2 = R$, and the conclusion follows.

§9.1 #42 Let R be the relation on the set $\{1, 2, 3, 4, 5\}$ containing the ordered pairs $(1, 1)$, $(1, 2)$, $(1, 3)$, $(2, 3)$, $(2, 4)$, $(3, 1)$, $(3, 4)$, $(3, 5)$, $(4, 2)$, $(4, 5)$, $(5, 1)$, $(5, 2)$ and $(5, 4)$. Find (a) R^2, (b) R^3, (c) R^4, (d) R^5.

The powers indicated are as follows:

$$R^2 = \{(1,1),(1,2),(1,3),(1,4),(1,5),(2,1),(2,2),(2,4),(2,5),(3,1),(3,2),(3,3),(3,4),(3,5),(4,1),$$
$$(4,2),(4,3),(4,4),(5,1),(5,2),(5,3),(5,4),(5,5)\} = \{1,2,3,4,5\}^2 - \{(2,3),(4,5)\}$$
$$R^3 = \{1,2,3,4,5\}^2 = R^4 = R^5.$$

Name: _____

§9.4 #29 Find the smallest relation containing the relation $\{(1,2),(1,4),(3,3),(4,1)\}$ that is

(a) reflexive and transitive

Since the transitive closure of a reflexive relation is reflexive, the transitive closure of the reflexive closure of the relation is the smallest relation that satisfies the condition: $\{(1,1),(1,2),(1,4),(2,2),(3,3),(4,1),(4,2),(4,4)\} \cup \{(a,a) \mid a \in S\}$.

(b) symmetric and transitive

Since the transitive closure of a symmetric relation is symmetric, the transitive closure of the symmetric closure of the relation is the smallest relation that satisfies the condition: $\{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(3,3),(4,1),(4,2),(4,4)\}$.

(c) reflexive, symmetric and transitive

Since the transitive closure of a symmetric relation that relates all the elements is also reflexive, the transitive closure of the symmetric closure of the relation is the smallest equivalence relation containing the relation, which partitions the: $\{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(3,3),(4,1),(4,2),(4,4)\} \cup \{(a,a) \mid a \in S\}$.

§9.5 #13 Let R be the relation on the set of ordered pairs of positive integers such that $((a,b),(c,d)) \in R$ if and only if $a+d=b+c$. Show that R is an equivalence relation.

For $a,b \in \mathbb{N}$, $a+b=b+a$, so $((a,b),(a,b)) \in R$, and R is reflexive. If $((a,b),(c,d)) \in R$, $a+d=b+c$, so $c+b=d+a$ and $((c,d),(a,b)) \in R$, and R is symmetric. If $((a,b),(c,d)) \in R$ and $((c,d),(e,f)) \in R$, then $a+d=b+c$ and $c+f=d+e$, so $a+d+c+f=b+c+d+e$, which gives $a+f=b+e$ by cancelling $c+d$, and $((a,b),(e,f)) \in R$, and R is transitive. Since R is reflexive, symmetric and transitive, R is an equivalence relation, with equivalence classes $[(n,1)]_R$ and $[(1,n)]_R$, where $n \in \mathbb{N}$.

§9.5 #43 Find the smallest equivalence relation on the set $\{a,b,c,d,e\}$ containing the relation $\{(a,b),(a,c),(d,e)\}$.

The smallest equivalence relation containing the given relation, which relates all elements of the given set, is the transitive closure of the symmetric closure of the relation—that is, the relation that partitions the set: $\{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c),(d,d),(d,e),(e,d),(e,e)\}$.

§9.6 #8 Let (S,R) be a poset. Show that (S,R^{-1}) is also a poset, where R^{-1} is the inverse of R. The poset (S,R^{-1}) is called the *dual* of (S,R).

Since (S,R) is a poset, R is reflexive, antisymmetric and transitive. Since R is reflexive, $(s,s) \in R$, for all $s \in S$, so $(s,s) \in R^{-1}$, for all $s \in S$, so R^{-1} is reflexive. If $a \neq b$, $(a,b) \in R^{-1}$ implies $(b,a) \in R$; since R is antisymmetric, $(a,b) \notin R$ so $(b,a) \notin R^{-1}$, and R^{-1} is antisymmetric. If $(a,b),(b,c) \in R^{-1}$, then $(c,b),(b,a) \in R$; since R is transitive, $(c,a) \in R$ and $(a,c) \in R^{-1}$, so R^{-1} is transitive. Since R^{-1} is reflexive, antisymmetric and transitive, R^{-1} is a partial order, and (S,R^{-1}) is a poset.

§9.6 #23 Answer these questions for the poset $(\{3,5,9,15,24,45\}, |)$.

(a) Find the maximal elements.

The maximal elements are 24 and 45.

(b) Find the minimal elements.

The maximal elements are 3 and 5.

(c) Is there a greatest element?

There is no element b such that $a \mid b$ for all elements a. In particular 24 and 45 are not comparable.

(d) Is there a least element?

There is no element a such that $a \mid b$ for all elements b. In particular 3 and 5 are not comparable.

(e) Find all upper bounds of $\{3,5\}$.

The upper bounds of $\{3,5\}$ are 15 and 45.

(f) Find the least upper bound of $\{3, 5\}$, if it exists.
Since $15 \mid 45$, 15 is the least upper bound of $\{3, 5\}$.

(g) Find all lower bounds of $\{15, 45\}$.
The lower bounds of $\{15, 45\}$ are 3, 5 and 15.

(h) Find the greatest lower bound of $\{15, 45\}$, if it exists.
Since $3 \mid 15$ and $5 \mid 15$, 15 is the greatest lower bound of $\{15, 45\}$.

Source: Kenneth Rosen and Kamala Krithivasan, *Discrete Mathematics and Its Applications*, 7th ed

Name: _____

§1.1 #35 The nth statement in a list of 100 statements is "Exactly n of the statements in this list are false."

(a) What conclusions can you draw from these statements?

The crucial observation is that since each statement says something that every other statement cannot agree with, *at most one statement is true*.

From that, there are only two possibilities:

- All the statements are false: Then the 100th statement is true, since that statement asserts that exactly 100 of the statements in the list are false. Thus, only 99 statements are false, which is a contradiction.
- Exactly one statement is true: then exactly 99 statements are false, which is asserted by the 99th statement, which is thus the only true statement in the list.

(b) Answer part (a) if the nth statement is "At least n of the statements in this list are false."

Unlike part (a), multiple statements can be true: if the nth statement is true, the $(n-1)$th statement is true—in fact, the first through the nth statements must be true.

If, instead, the nth statement is false, then less than n of the statements are false, so more than $100 - n$ statements must be true—in that case, there can't be $n + 1$ false statements, and, in fact, the nth through the 100th statements must be false.

If the nth statement is true, and the $(n + 1)$ is false, then there has to be exactly n false statements, which have to be the $(n + 1)$th statement through the 100th statement. Thus, $100 = n + n$, and $n = 50$. So, the first fifty statements are true, while the last fifty statements are false.

(c) Answer part (b) assuming that the list contains 99 statements.

Following the reasoning in part (b), $99 = n + n$, where the first n statements are true, and the last n statements are false. This does not work out: if the first forty-nine statements are true, and the last forty-nine statements are false, the 50th statement would contradict itself whether or not it was true. Thus, there is no truth assignment to all 99 statements that would be satisfactory.

§1.2 #11 When three professors are seated in a restaurant, the hostess asks them: "Does everyone want coffee?"

The first professor says: "I do not know."

The second professor then says: "I do not know."

Finally, the third professor says: "No, not everyone wants coffee."

The hostess comes back and gives coffee to the professors who want it. How did she figure out who wanted coffee?

Consider the question as answerable by yes or no, dependent on the preference of each professor, and the information each preceding professor provides by their answer:

- If the first professor does not want coffee, then the professor can reply definitively say "no" (as the third professor does), since at least one professor does not want coffee. Since the first professor does not say "no", the first professor wants coffee—the answer indicates that the first professor wants coffee, and is unsure if the other two professors both want coffee.
- Knowing that the first professor wants coffee, by similar reasoning, the second professor wants coffee, but is unsure if the third professor wants coffee.
- The third professor already knows that the first and second professors both want coffee, and the answer indicates the third professor's preference—thus, the third professor does not want coffee.

§1.4 #25 Express each of these statements using predicates and quantifiers.

(a) A passenger of an airline qualifies as an elite flyer if the passenger flies more than 25000 miles in a year or takes more than 25 flights during that year.

If the predicate $E(p)$ asserts that passenger p qualifies as an elite flyer, the predicate $M(p, y)$ asserts that passenger p flies more than 25000 miles in the year y, and the predicate $F(p, y)$

asserts that passenger p takes more than 25 flights during the year y, then the statement can be written as $\forall p \exists y[(M(p,y) \vee F(p,y)) \rightarrow E(p)]$, where p is over the domain of all passengers of the airline, and y is over the domain of all years that the airline has had flights.

(b) A man qualifies for the marathon if his best previous time is less than 3 hours and a woman qualifies for the marathon if her best previous time is less than 3.5 hours.

If the predicate $Q(x)$ asserts that person x qualifies for the marathon, the predicate $M(x)$ asserts that person x is a man, the predicate $W(x)$ (for binary gender, this would be equivalent to $\neg M(x)$) asserts that person x is a woman, and the predicate $T(x,t)$ asserts the best previous time of person x is less than t hours, then the statement can be written as $\forall x([(M(x) \wedge T(x,3)) \vee (W(x) \wedge T(x,3.5))] \rightarrow Q(x))$, where x is over the domain of persons that can qualify for the marathon (as there may be other restrictions).

(c) A student must make at least 60 course hours, or at least 45 course hours and write a master's thesis, and receive a grade no lower than a B in all required courses, to receive a master's degree.

If the predicate $M(s)$ asserts that student s receives a master's degree, the predicate $C(s,h)$ asserts that student s makes at least h course hours, the predicate $T(s)$ asserts that student s writes a master's thesis, and the predicate $G(s,c,g)$ asserts that student s received a grade of g or higher for course c, then the statement can be written as $\forall s[M(s) \rightarrow ([C(s,60) \vee (C(s,45) \wedge T(s))] \wedge [\forall c G(s,c,B)])]$, where s is over the domain of students that can receive a master's degree, and c is over the domain of courses required for that student s.

(d) These is a student who has taken more than 21 credit hours in a semester and received all As.

If the predicate $C(s,h,t)$ asserts that student s has taken more than h credit hours in semester t, and the predicate $G(s,c,g)$ asserts that student s received a grade of g or higher for course c, and if A is the highest grade, then the statement can be written as $\exists s \exists t[C(s,21,t) \wedge (\forall c G(s,c,A))]$, where s is over the domain of students that considered, and c is over the domain of courses that student s took in the semester t.

§1.5 #21 Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.

(a) $\forall x \forall y(x^2 = y^2 \rightarrow x = y)$

The statment asserts that for any two integers, if the squares of the integers are equal, then the integers are equal. A counterexample is for $x = -y$: $x^2 = (-y)^2 = y^2$, but, if $x \neq 0$, $x \neq y$.

(b) $\forall x \exists y(y^2 = x)$

The statment asserts that any integer is the square of another integer. A counterexample is for a nonsquare x, such as $x = 2$: there is no integer y such that $y^2 = 2$; also, for every negative integer x, there is no integer y whose square is a negative number.

(c) $\forall x \forall y(xy \geq x)$

The statment asserts that the product of any two integers is greater than or equal to the first integer. A counterexample is for positive integers x, if $y \leq 0$, $xy \leq 0 < x$; another counterexample is for negative integers x, if $y \geq 1$, $xy < x$.

⋆ From Raymond Smullyan, *The Gödelian Puzzle Book: Puzzles, Paradoxes & Proofs*:

A logician once visited a very strange island in which not every inhabitant was either a knight (who always told the truth) or knave (who always lied). Those who were neither one were called outcasts. An outcast would lie on some days and be truthful on others. On any day, he would either lie the entire day, or be truthful the entire day, but his behavior could change from day to day. On a given day, to say that a person is *currently* truthful is to say that he is either a knight (who is truthful on all days) or that he is an outcast and that day is one of his truthful days.

The logician was captured by a tribe of bandits. Curiously enough, the chief bandit was a knight, and this fact was common knowledge. He had been interested in logic and loved to test his victims. And so he led the logician into a room with nine natives and explained that only one of them was a knight—each one of the other eight was either a

knave or an outcast. The logician's task was to determine which one was the knight. If he succeeded, he would be set free; otherwise, he would be executed. Here is what the nine men said.

Archie	The knight is either Cary, Elmak, Greg or myself.
Barab	I am an outcast.
Cary	Either Elmak is currently truthful or Greg is not.
Dreg	Archie lied.
Elmak	Barab and Dreg didn't both lie.
Frisch	Cary lied.
Greg	Archie is not the knight.
Hal	I am a knave and Ilak is an outcast.
Ilak	I am a knave and Frisch lied.

The logician thought about this for while and finally said, "I don't have enough information to solve the problem. I need to know whether or not Hal is an outcast. Then I might be able to solve it." The chief bandit was fair enough to tell him whether or not Hal was an outcast, and the logician could then figure out which one was the knight. Which one was the knight?

Since, for each of the nine natives, there are four possibilities (the native is a knight, a knave, an outcast who is telling the truth that day, or an outcast who is lying that day), a comprehensive "truth" table would have $4^9 > 250000$ entries, so it is not ideal to use satisfiability to find the answer. To simplify matters, consider the essential question: who *can be* the knight?

Three natives cannot be the knight on the basis of their statement, as a knight cannot lie: Barab, Hal and Ilak—Hal and Ilak have to be lying (their statements assert that they are knaves, who always lie, so their statements cannot be true), while Barab can be a truth-telling outcast, or a (lying) knave.

Related to this, it is most crucial to determine the truth or falsehood of Frisch's statement.

- Can Frisch be the knight?
  - *If Frisch told the truth*, Cary lied (and is not the knight).
  - *If Cary lied*, Elmak lied (and is not the knight) and Greg told the truth.
  - *If Elmak lied*, Barab lied (and is a knave) and Dreg lied (and is not the knight).
  - *If Dreg lied*, Archie told the truth.
  - *If Greg told the truth*, Archie is not the knight.
  - *If Archie told the truth and none of Archie, Cary or Elmak is the knight*, Greg is the knight.

  So Frisch cannot be the knight.
- For each of the other natives to be the knight:
  - If Archie is the knight, Greg lied, so Cary told the truth.
  - If Dreg is the knight, Elmak told the truth, so Cary told the truth.
  - If Elmak is the knight, Cary told the truth.
  - If Cary is the knight or if Cary told the truth, Frisch lied.

So *if Frisch told the truth, Greg is the knight*, but *if any of Archie, Cary, Dreg or Elmak is the knight, Frisch lied*.

Now consider the lies of Hal and Ilak:

- *If Frisch lied*, since Ilak lied, Ilak cannot be a knave, so Ilak must be an outsider.
- *If Ilak is an outsider*, since Hal lied, Hal cannot be a knave, so Hal must be an outsider.

So *if Frisch lied, Hal is an outsider*. Therefore, *if Hal is not an outsider (thus is a knave), Frisch told the truth*.

The metapuzzle is that the bandit chief told the logician whether Hal was an outsider or not. If the bandit chief told the logician that Hal was an outsider, the logician would not be able to tell who

the knight was. (Hal is an outsider if any of Archie, Cary, Dreg or Elmak is the knight. It is possible that Frisch told the truth and Hal is an outsider—then it would not be possible to determine if Ilak was an outsider or a knave—and Greg would be the knight.) However, if the bandit chief told the logician that Hal was not an outsider, then the logician would conclude that Hal is a knave. Since *knowing whether or not Hal was an outsider was sufficient for the logician to determine the knight*, Hal must not be an outsider, and the knight is Greg.

Source: Kenneth Rosen and Kamala Krithivasan, *Discrete Mathematics and Its Applications*, 7th ed

Name: _____

§1.8 #19 Are these steps for finding the solutions of $\sqrt{x+3} = 3 - x$ correct?

(1) $\sqrt{x+3} = 3 - x$ is given
(2) $x + 3 = x^2 - 6x + 9$, obtained by squaring both sides of (1)
(3) $0 = x^2 - 7x + 6$, obtained by subtracting $x + 3$ from both sides of (2)
(4) $0 = (x - 1)(x - 6)$, obtained by factoring the right-hand side of (3)
(5) $x = 1$ or $x = 6$, which follows from (4) because $ab = 0$ implies that $a = 0$ or $b = 0$

The spurious answer $x = 6$ arises from (2), which ignores the restrictions $3 - x \geq 0$ and $3 + x \geq 0$ or $-3 \leq x \leq 3$ in (1).

§1.8 #21 Prove that if n is an integer, these four statements are equivalent:

(a) n is even,
(b) $n + 1$ is odd,
(c) $3n + 1$ is odd,
(d) $3n$ is even.

The following sequence of proofs is sufficient, noting $n \in \mathbb{Z}$:

- If n is even, then $n + 1$ is odd: directly, $n = 2k$, where $k \in \mathbb{Z}$; $n + 1 = 2k + 1$, thus $n + 1$ is odd.
- If $n+1$ is odd, then $3n+1$ is odd: directly, $n+1 = 2k+1$, where $k \in \mathbb{Z}$; $3n+1 = 2n+2k+1 = 2(n + k) + 1$, and $n + k \in \mathbb{Z}$, thus $3n + 1$ is odd.
- If $3n + 1$ is odd, then $3n$ is even: directly, $3n + 1 = 2k + 1$, where $k \in \mathbb{Z}$; $3n = 2k$, thus $3n$ is even.
- If $3n$ is even, then n is even: indirectly, if n is odd, $n = 2k+1$, $k \in \mathbb{Z}$; $3n = 6k+3 = 2(3k+1)+1$, and $3k + 1 \in \mathbb{Z}$, thus $3n$ is odd—as a contrapositive, this implies if $3n$ is even, then n is even.

§1.9 #5 Prove that there are 100 consecutive positive integers that are not perfect squares. Is your proof constructive or non-constructive?

A constructive proof: since $(n + 1)^2 - n^2 = 2n + 1$, when $2n + 1 > 100$, the consecutive perfect squares n^2 and $(n + 1)^2$ have $2n$ consecutive integers $n^2 + k$, $1 \leq k \leq 2n$, which are not perfect squares, when $n \geq 50$. Thus, $50^2 + k$, $1 \leq k \leq 100$—or 2501–2600, are not perfect squares.

§1.9 #15 Prove that given a real number x there exist unique numbers n and ε such that $x = n - \varepsilon$, n is an integer, and $0 \leq \varepsilon < 1$.

By definition, $\lfloor x \rfloor$ (the greatest integer function) is an integer for all real numbers x, with $0 \leq x - \lfloor x \rfloor < 1$—let $n = \lceil x \rceil = \begin{cases} x, & \text{if } x \in \mathbb{Z}, \\ \lfloor x \rfloor + 1, & \text{otherwise,} \end{cases}$ and $\varepsilon = n - x$. If there is another pair n', ε' satisfying $n' \in \mathbb{Z}$, $x + \varepsilon' = n$ and $0 \leq \varepsilon' < 1$, then $x = n - \varepsilon = n' - \varepsilon'$ gives $n - n' = \varepsilon - \varepsilon'$—the left-hand side is the difference of two integers, and is an integer, but $-1 < \varepsilon - \varepsilon' < 1$. Thus, $\varepsilon - \varepsilon' = 0$, $\varepsilon = \varepsilon'$ and $n = x + \varepsilon = x + \varepsilon' = n'$, so n and ε are unique (by §1.9 #11 (c)).

§1.9 #19 Prove that between every two rational numbers there is an irrational number.

Given two distinct rational numbers a and b, $a < b$, consider $c = \dfrac{a}{\sqrt{2}} + \dfrac{b(\sqrt{2} - 1)}{\sqrt{2}}$: $c = at + b(1 - t)$ for $0 < t = \dfrac{1}{\sqrt{2}} < 1$, so $a < c < b$, and $c = a + t(b - a)$.

If $c \in \mathbb{Q}$, then $c - a \neq 0$ and $b - a$ are rational, so $\sqrt{2} = \dfrac{b - a}{c - a}$ is rational, which is a contradiction. So c is an irrational number between rational numbers a and b.

Source: Kenneth Rosen and Kamala Krithivasan, *Discrete Mathematics and Its Applications*, 7th ed