1. **Predicates** [12 points]

Suppose three predicates, C, D and O (standing for being a cat, a dog, or the name of an operating system) are defined over the universe {Lion, Wolf, Fox, Puma, Jaguar}, as follows (T denotes True and F denotes False).

x	$C(x)$	$D(x)$	$O(x)$
Lion	T	F	T
Wolf	F	T	F
Fox	F	T	F
Puma	T	F	F
Jaguar	T	F	T

Select all the statements below that are true. (No justification is needed.)

☑ A. $\forall x\ O(x) \to C(x)$. [+4]
Since C(Lion) and C(Jaguar).

☐ B. $\exists x\ \neg(O(x) \to C(x))$. [−4]
This is the negation of A.

☑ C. $\exists x\ D(x) \to O(x)$. [+4]
consider x s.t. $\neg D(x)$: say $x =$ Lion.

☑ D. $\forall x\ \neg(C(x) \wedge D(x))$. [+4]
C and D are never simultaneously true.

2. **Functions** [12 points]

In this problem, we denote the set of 2-bit strings by S. That is, $S = \{00, 01, 10, 11\}$. We define two functions related to this set.

The function f takes two 2-bit strings x and y and returns a 2-bit string which indicates in which positions x and y differ, as in the following examples: $f(10, 10) = 00$ since the two strings are identical; $f(11, 10) = 01$ since 11 and 10 differ only in the last bit; $f(10, 01) = 11$ since the two strings differ in both positions; etc.

The function g takes a 2-bit string and returns the number of 1s in the string. The function table for g is given below.

x	$g(x)$
00	0
01	1
10	1
11	2

Answer the following questions about f and g as defined above.

(a) What are the domain and co-domain of f? [3 points]

☐ A. Domain is S and co-domain S. [−3]

☐ B. Domain is S and co-domain $S \times S$. [−3]

☑ C. Domain is $S \times S$ and co-domain is S. [+3]

☐ D. Domain is $S \times S$ and co-domain is $S \times S$. [−3]

(b) What is the image of g? [3 points]

$$\text{Image}(g) = \{ \quad 0,\ 1,\ 2 \quad \}.$$

(c) What is $f \circ g(x)$? [3 points]

☐ A. The number of 1s in the string x. [−3]

☐ B. The string 000. [−3]

☐ C. The number 0. [−3]

☑ D. $f \circ g$ is not a well-defined function. [+3]

(d) What is $g \circ f(x, y)$? [3 points]

☐ A. The number of 1s in the two strings x and y. [−3]

☐ B. A 2-bit string in which each bit is the XOR of the corresponding bits in the strings x and y. [−3]

☑ C. The number of positions x and y differ in. [+3]

☐ D. $g \circ f$ is not a well-defined function. [−3]

3. **Multiple Choice Problems.** [24 points]

This page has 4 problems, each worth 6 points. Each problem has one or more correct choices. **For full credit, you should select all the correct choices and none of the wrong choices.**

I. **Sets.** [6 points]

For any sets A, B, C, we have $A \cap B \cap C =$

☐ A. $\overline{A \cup B \cup C}$ [−2]

☐ B. $A \cap (B - C)$ [−2]

☑ C. $(A \cap B) - \overline{C}$ [+6]

☐ D. $(A \cap B) \cup (A \cap C)$ [−2]

II. **Remainder.** [6 points]

Given integers a, b where $b > 0$, the remainder obtained on dividing a by b equals:

☐ A. $b\lceil a/b \rceil - a$ [−2]

☑ B. $a - b\lfloor a/b \rfloor$ [+6]

☐ C. $b - a\lfloor b/a \rfloor$ [−2]

☐ D. $a\lceil b/a \rceil - b$ [−2]

III. **Modular Arithmetic.** [6 points]

Consider an arbitrary integer $m > 1$. Then select all the numbers a such that $a^2 \equiv 1 \pmod{m}$, from the following options.

☑ A. $a = m + 1$ [+2]

☑ B. $a = 2m + 1$ [+2]

☑ C. $a = m - 1$ [+2]

☐ D. $a = m$ [−2]

IV. **Counting.** [6 points]

How many distinct predicates exist over the universe A, if $|A| = n$? (Recall that a predicate over A is a function $f : A \to \{T, F\}$.)

☐ A. n [−6]

☐ B. n^2 [−6]

☐ C. $n!$ [−6]

☑ D. 2^n [+6]

4. **Relations.** [6 points]

Suppose $f : A \to B$, where $A = B = \{0, 1, 2, 3, 4, 5, 6\}$, defined as $f(x) = \lfloor x/2 \rfloor$. Define the relation $\sim$ (over the elements of A) as follows:

$$x \sim y \text{ if and only if } f(x) = f(y).$$

Then $\sim$ is an equivalence relation. (You don't have to prove this.) List the equivalence classes of $\sim$.

Solution: The equivalence classes are: $\{0, 1\}, \{2, 3\}, \{4, 5\}, \{6\}$.

5. **Euclidean Algorithm** [6 points]

Execute the Euclidean algorithm for finding the gcd of 300 and 51. Show all the intermediate values of the variables. Clearly indicate what the final result is.

Solution: Below, $r = \text{remainder}(x, y)$ is the remainder on dividing x by y.

x	y	r
300	51	45
51	45	6
45	6	3
6	3	0

$\gcd(300, 51) = 3$.

6. **Congruence and Modular Arithmetic.** [10 points]

(a) The goal of this part of the problem is to make sure that you recall the definition of congruence. For integers a, b, m, define the congruence $a \equiv b \pmod{m}$ in terms of the "divides" relation. (Recall that $x|y$ is said to hold if $\exists z \in \mathbb{Z},\ y = xz$). [4 points]

Solution: For integers a, b, m, we define $a \equiv b \pmod{m}$ if $m|(a-b)$.

(b) Prove that for all positive integers a, b and m, if $a \equiv b \pmod{m}$, then $a^3 \equiv b^3 \pmod{m}$. [6 points]

Solution: Let a, b, m be arbitrary (positive) integers s.t. $a \equiv b \pmod{m}$. Hence $m|(a-b)$. Since $(a^3 - b^3) = (a-b)(a^2+ab+b^2)$, we have $(a-b)|(a^3-b^3)$. Then, by the transitivity of the divides relation, we have $m|(a^3-b^3)$. Thus by definition, $a^3 \equiv b^3 \pmod{m}$. Since a, b, m were arbitrarily chosen integers, we have shown that for all (positive) integers $a, b, m,$, if $a \equiv b \pmod{m}$, then $a^3 \equiv b^3 \pmod{m}$.

Alternately, since $m|(a-b)$, there is an integer k s.t. $a - b = mk$. So $a = b + mk$, and therefore $a^3 = (b+mk)^3 = b^3+3b^2mk+3b(mk)^2+(mk)^3 = b^3+m(3b^2k+3bmk^2+m^2k^3)$. Thus $a^3-b^3 = m\ell$, where $\ell = (3b^2k + 3bmk^2 + m^2k^3)$ is an integer. Thus $m|(a^3 - b^3)$. Thus by definition, $a^3 \equiv b^3 \pmod{m}$.

7. **English to Logic.** [15 points]

In 1742, Christian Goldbach communicated to Leonhard Euler the following deceptively simple *conjecture*, which remains unproven to this day.

> **Goldbach's Conjecture.** Every even integer greater than 2 can be expressed as the sum of two primes.

(a) Write this conjecture as a statement in predicate logic, using the predicates Even and Prime, where the universe is the set of integers $\mathbb{Z}$; you can also use familiar mathematical relations and operators $=, \geq, +$ etc. [8 points]

Solution:

$$\forall x \in \mathbb{Z}, \exists a, b \in \mathbb{Z} \ \big(\text{Even}(x) \wedge x > 2\big) \rightarrow \big(\text{Prime}(a) \wedge \text{Prime}(b) \wedge (x = a + b)\big)$$

Alternately,

$$\forall x \in \mathbb{Z} \ \big(\text{Even}(x) \wedge x > 2\big) \rightarrow \exists a, b \in \mathbb{Z}\big(\text{Prime}(a) \wedge \text{Prime}(b) \wedge (x = a + b)\big).$$

(b) Then verify that this statement is true if instead of $\mathbb{Z}$, the universe is restricted to $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. [7 points]

Solution: The statement is vacuously true for $x = 0, 1, 2, 3, 5, 7$. (Explanation not needed.) For $x = 4$, pick $a = b = 2$. For $x = 6$, pick $a = b = 3$. For $x = 8$ pick $a = 5, b = 3$.

8. **Relations.** [15 points]

Given two relations R_1 and R_2 over the set A, we can define a new relation R^* as follows: for every $x, y \in A$,

$$(x, y) \in R^* \text{ if and only if } (x, y) \in R_1 \text{ or } (x, y) \in R_2.$$

As an example, if R_1 is the $<$ relation among integers and R_2 is the $=$ relation, then R^* would be the $\leq$ relation.

For each of the following statements, either indicate that it is true (irrespective of what R_1, R_2 are) or not. If true, briefly justify; if not, give a counter-example for which it is false (you can define suitable relations R_1, R_2 for your counter-examples):

(a) if R_1 is reflexive, then R^* is reflexive. [7 points]

Solution:: True. Since, for all x, $(x, x) \in R_1$ and $R^* = R_1 \cup R_2$, we have $(x, x) \in R^*$.

(b) if R_1 and R_2 are both anti-symmetric, then R^* is anti-symmetric. [8 points]

Solution:: False. e.g., suppose R_1 is anti-symmetric (say $<$) and R_2 is its complement (in this case, $\geq$), then R^* is the complete relation such that $\forall x, y \ (x, y) \in R^*$. This relation is not anti-symmetric.

(Other examples possible. Graph representation of the relation is fine.)

9. **Extra Credit.** [15 points]

Recall that for two positive integers a, b we can express their LCM as $\text{lcm}(a, b) = ab/\gcd(a, b)$. Derive an analogous expression for $\text{lcm}(a, b, c)$ (for $a, b, c \in \mathbb{Z}^+$) in terms of a, b, c, $\gcd(a, b)$, $\gcd(b, c)$, $\gcd(c, a)$ and $\gcd(a, b, c)$.

[Hint: Recall the prime factorization of n represented using the set $PF_n = \{(p, i)|p \text{ prime and } i \in \mathbb{Z}^+ \text{ s.t. } (p^i)|n\}$. Follow the analogy of the inclusion-exclusion principal for three sets.]

Solution:

$$\text{lcm}(a, b, c) = \frac{a \cdot b \cdot c \cdot \gcd(a, b, c)}{\gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(c, a)}.$$