1. [8 points] Let $P(x)$ and $Q(x)$ be predicates where the universe of discourse for $x$ is some set $U$. Let $A = \{x : P(x) \text{ is true}\}$ and let $B = \{x : Q(x) \text{ is true}\}$ be the truth sets of $P(x)$ and $Q(x)$, respectively.

Circle all the predicates below that have truth set equal to $A \cap B$?

(a) YES $P(x) \land \neg Q(x)$
(b) YES $\neg(P(x) \rightarrow Q(x))$
(c) YES $\neg(\neg P(x) \lor Q(x))$
(d) $\neg(Q(x) \lor P(x))$
(e) $\neg(P(x) \land Q(x))$

2. [8 points] Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions where $A, B, C$ are finite sets. Circle all the CORRECT statements below.

(a) If $f$ is surjective, then $|A| \leq |B|$.
(b) If $|A| \leq |B|$, then $f$ is injective.
(c) YES If $f$ is surjective and $|A| = |B|$, then $f$ is injective
(d) YES If $f$ and $g$ are both injective, then $g \circ f$ is injective.
(e) If $g$ is surjective, then $g \circ f$ is surjective.
3. [8 points] Circle all the CORRECT statements below, or circle (e):

(a) YES \([-n] = -[n]\).

(b) \([-2.999999999]\) = -3

(c) \([x + y] = [x] + [y]\)

(d) YES \([x - 0.5]\) is the closest integer to \(x\), rounding down in the case of ties.

(e) None are correct.

4. [6 points] The number of different functions \(f : A \rightarrow B\) from a set \(A\) of \(m\) elements to a set \(B\) of \(n\) elements equals:

(a) \(mn\)

(b) YES \(n^m\)

(c) \(m^n\)

(d) \(m + n\)

(e) None of the above

5. [10 points] For each of the functions \(f(n)\) below, give the simplest function \(g(n)\) such that \(f(n) = \Theta(g(n))\).

(a) \(.01n^3 - 1000n^2 + 5n + 35\): \(\Theta(n^3)\)

(b) \(\frac{4n^5 + 3n^4 \log n - 3n + 5}{2n^3 + 5n^2 - 6n + 8}\): \(\Theta(n^2)\)

(c) \(f(n) = [n]n\): \(\Theta(n^2)\)

(d) \(f(n) = \sin n\): \(\Theta(1)\)
6. [10 points] What is the conjunctive normal form (that is, product of sums) of the Boolean function \( f(x, y, z) \) of three Boolean variables \( x, y, z \) that equals 0 if and only if \( x = 0, y = 1, z = 0 \), or \( x = 1, y = 0, z = 0 \), or \( x = 1, y = 1, z = 1 \).

\[
(x + \bar{y} + z)(\bar{x} + y + z)(\bar{x} = \bar{y} + \bar{z}).
\]

7. [10 points] Prove by mathematical induction that the sum of the first \( n \) odd positive integers is \( n^2 \), that is,

\[
P(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2, \quad (n \geq 1).
\]

**Basis Step:** \( P(1) \) holds. \( 1 = 1^2 = 1 \) OK

**Inductive Step:** \( P(n) \rightarrow P(n + 1) \) for each \( n \geq 1 \)

Assume \( T \) \( P(n) \) : \( 1 + 3 + 5 + \cdots + (2n - 1) = n^2 \)

Prove \( T \) \( P(n + 1) \) : \( 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = (n + 1)^2 \)

We have: \( 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = (1 + 3 + 5 + \cdots + (2n - 1)) + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2 \), since \( P(n) \) is true.

So \( P(n + 1) \) is \( T \), and the formula follows by math induction.

8. [10 points] Compute a simple closed form expression for the sum

\[
\sum_{i=0}^{m} \sum_{j=0}^{n} 5^i(3 + 2j).
\]

\[
\sum_{i=0}^{m} \sum_{j=0}^{n} 5^i(3 + 2j).
\]

Using formulas for geometric and arithmetic sequences, we have

\[
\sum_{i=0}^{m} \sum_{j=0}^{n} 5^i(3 + 2j) = \sum_{i=0}^{m} 5^i \sum_{j=0}^{n} (3 + 2j) = \frac{5^{m+1} - 1}{4} \left(3(n + 1) + 2 \frac{n(n + 1)}{2} \right)
\]

9. [10 points] Alice wants to send Bob a secure message via the RSA cryptosystem. She looks on his webpage and finds Bob’s RSA modulus \( n = 33 \) and \( e = 3 \). What Alice can **not** see is that on Bob’s private page is \( 33 = 3 \cdot 11 \) and that Bob has also chosen an integer \( d = 7 \).

(a) Verify that \( d \) has the required property for RSA.

Need \( e \cdot d \) congruent to 1 modulo 20 where \( 20 = (3 - 1) \cdot (11 - 1) \). But \( 3 \times 7 = 21 \) and this is so.
(b) Alice wants to send Bob the important message 5. Compute the encrypted message (an integer between 1 and 32) that she sends?

\[ c = 5^3 \mod 33 \text{ and this is 26.} \]

(c) April, a different friend of Bob, has sent Bob a message which he received as 2. What message (an integer between 1 and 32) did April send Bob?

This is \[ m = 2^7 \mod 33 \text{ which equals 29.} \]

10. [10 points]
(a) If it exists, use the Euclidean Algorithm to find the multiplicative inverse of 14 modulo 45 (trial and error not acceptable).

We get

\[
45 = 3 \cdot 14 + 3 \\
14 = 4 \cdot 3 + 2 \\
3 = 1 \cdot 2 + 1 \\
2 = 2 \cdot 1 + 0
\]

So GCD is 1 and an inverse exists. Using the equations in the reverse order we get that

\[ 1 = 5 \cdot 45 - 16 \cdot 14 \]

Since \(-16\) is 29 modulo 45, we get the inverse to be 29.

(b) Use your answer above — calculator answer not acceptable — to find a solution to \[ 14x \equiv 47 \mod 45 \text{ where } x \text{ is between 0 and 44} \].

\[ x = 29 \cdot 47 \text{ or } 29 \cdot 2 \text{ or 58 which is 13 modulo 45.} \]

11. [10 points] Give a proof by contradiction that if \(a\) and \(b\) are nonnegative numbers, then

\[
\frac{a + b}{2} \geq \sqrt{ab}.
\]

Suppose not. Then

\[
\frac{a + b}{2} < \sqrt{ab}
\]

Squaring we get

\[
\frac{a^2 + 2ab + b^2}{4} < ab
\]

This gives \(a^2 + 2ab + b^2 < 4ab\) or \(a^2 - 2ab + b^2 < 0\) or \((a - b)^2 < 0\), a contradiction since a square is always at least zero.