Midterm 1 Sample Solutions
Problem 1. [True or false] (20 points)

(a) **True** or **False**: Let the logical proposition \( R(x) \) be given by \( x^2 = 4 \implies x \leq 1 \). Then \( R(3) \) is true.

(\textit{False implies anything.})

(b) **True** or **False**: The proposition \( P \implies (P \land Q) \) is logically equivalent to \( P \implies Q \).

(c) **True** or **False**: The proposition \( P \implies (P \land Q) \) is logically equivalent to \( (P \land Q) \implies P \).

(Consider \( P = \text{True}, Q = \text{False} \).)

(d) **True** or **False**: The proposition \( (P \land Q) \lor (\neg P \lor \neg Q) \) is a tautology, i.e., is logically equivalent to True.

(e) **True** or **False**: \( \exists n \in \mathbb{N} \cdot (P(n) \land Q(n)) \) is logically equivalent to \( (\exists n \in \mathbb{N} \cdot P(n)) \land (\exists n \in \mathbb{N} \cdot Q(n)) \).

(Consider the propositions \( P(n) = \text{“n is odd”} \) and \( Q(n) = \text{“n is even”} \).

(f) **True** or **False**: \( \exists n \in \mathbb{N} \cdot (P(n) \lor Q(n)) \) is logically equivalent to \( (\exists n \in \mathbb{N} \cdot P(n)) \lor (\exists n \in \mathbb{N} \cdot Q(n)) \).

(g) **True** or **False**: \( \forall n \in \mathbb{N} \cdot ((\exists k \in \mathbb{N} \cdot n = 2k) \lor (\exists k \in \mathbb{N} \cdot n = 2k + 1)) \).

(Every natural number is either odd or even.)

(h) **True** or **False**: \( \exists n \in \mathbb{N} \cdot (\forall k \in \mathbb{N} \cdot n = 2k) \lor (\forall k \in \mathbb{N} \cdot n = 2k + 1)) \).

(For any \( n \in \mathbb{N} \), take \( k = 100n + 100 \); then \( n \not= 2k \) and \( n \not= 2k + 1 \).)

(i) **True** or **False**: \( \forall n \in \mathbb{N} \cdot ((\exists k \in \mathbb{N} \cdot n = k^2) \implies (\exists \ell \in \mathbb{N} \cdot n = \sum_{i=1}^{\ell} (2i - 1))) \).

(For any \( n \in \mathbb{N} \) with \( n = k^2 \), take \( \ell = k \).)

(j) **True** or **False**: If we want to prove the statement \( x^2 \leq 1 \implies x \leq 1 \) using Proof by Contrapositive, it suffices to prove the statement \( x^2 > 1 \implies x > 1 \).

(Converse error. We’d need to prove \( x > 1 \implies x^2 > 1 \).)

(k) **True** or **False**: If we want to prove the statement \( x^2 \leq 1 \implies x \leq 1 \) using Proof by Contradiction, it suffices to start by assuming that \( x^2 \leq 1 \land x > 1 \) and then demonstrate that this leads to a contradiction.

(\( x^2 \leq 1 \land x > 1 \) is the negation of \( x^2 \leq 1 \implies x \leq 1 \).)

(l) **True** or **False**: Let \( S = \{ x \in \mathbb{Z} : x^2 \equiv 2 \pmod{7} \} \). Then the well ordering principle guarantees that \( S \) has a smallest element.

(\( S \) is not a subset of the natural numbers, so the well ordering principle guarantees nothing. In fact, \( S \) has no smallest element, since \( x = 3 - 7n \) satisfies \( x^2 \equiv 2 \pmod{7} \) for every \( n \in \mathbb{N} \).)

(m) **True** or **False**: Let \( T = \{ n \in \mathbb{N} : n^2 \equiv 2 \pmod{8} \} \). Then the well ordering principle guarantees that \( T \) has a smallest element.

(\( T \) is the empty set, so the well ordering principle guarantees nothing in this case.)

(n) Suppose that, on day \( k \) of some execution of the Traditional Marriage Algorithm, Alice likes the boy who she currently has on a string better than the boy who Betty has on a string.

**True** or **False**: It’s guaranteed that on every subsequent day, this will continue to be true.

(Tomorrow, Betty might receive a proposal from some third boy who Alice has a mad crush on.)
Problem 2. [You complete the proof] (10 points)

The algorithm $A(\cdot, \cdot)$ accepts two natural numbers as input, and is defined as follows:

$A(n, m)$:
1. If $n = 0$ or $m = 0$, return 0.
2. Otherwise, return $A(n - 1, m) + A(n, m - 1) + 1 - A(n - 1, m - 1)$.

Fill in the boxes below in a way that will make the entire proof valid.

**Theorem:** For every $n, m \in \mathbb{N}$, we have $A(n, m) = nm$.

**Proof:** If $s \in \mathbb{N}$, let $P(s)$ denote the proposition 

\[ \forall n, m \in \mathbb{N} . n + m = s \implies A(n, m) = nm. \]

We will use a proof by strong induction on the variable $s$.

**Base case:** $A(0, 0) = 0$, so $P(0)$ is true.

**Inductive hypothesis:** Assume $P(0) \land \cdots \land P(s)$ (or: $\forall m, n \in \mathbb{N} . n + m \leq s \implies A(n, m) = nm$) is true for some $s \in \mathbb{N}$.

**Induction step:** Consider an arbitrary choice of $n, m \in \mathbb{N}$ such that $n + m = s + 1$. If $n = 0$ or $m = 0$, then $A(n, m) = 0 = nm$ is trivially true, so assume that $n \geq 1$ and $m \geq 1$. In this case we see that

\[
A(n, m) = A(n - 1, m) + A(n, m - 1) + 1 - A(n - 1, m - 1)
\]

(by the definition of $A(n, m)$)

\[
= (n - 1)m + n(m - 1) + 1 - (n - 1)(m - 1)
\]

(by the inductive hypothesis)

\[
= nm - m + nm - n + 1 - nm + n + m - 1
\]

\[
= nm.
\]

In every case where $n + m = s + 1$, we see that $A(n, m) = nm$. Therefore $P(s + 1)$ follows from the inductive hypothesis, and so the theorem is true. \qed

*Comment:* Simple induction is not good enough. In the induction step we need to know that $A(n - 1, m - 1) = (n - 1)(m - 1)$. Since $n - 1 + m - 1 = s - 1$, to prove $P(s + 1)$ we need to know that both $P(s)$ and $P(s - 1)$ are true.
Problem 3. [Modular arithmetic] (10 points)

Suppose that \( x, y \) are integers such that
\[
3x + 2y = 0 \pmod{71}
\]
\[
2x + 2y = 1 \pmod{71}
\]
Solve for \( x, y \). Find all solutions. Show your work. Circle your final answer showing all solutions for \( x, y \).

Solution: There are many ways to solve this. Here is one. First, isolate \( x \) by subtracting the 2nd equation from the 1st, yielding
\[
x \equiv -1 \pmod{71}.
\]
Plug this expression for \( x \) into the first original equation to get
\[
3 \times -1 + 2y \equiv 0 \pmod{71},
\]
i.e.,
\[
2y \equiv 3 \pmod{71}.
\]
Now \( \gcd(2, 71) = 1 \), so 2 has a multiplicative inverse modulo 71. One way to solve the equation for \( y \) is to notice that
\[
2y \equiv 3 + 71 \equiv 74 \pmod{71},
\]
and
\[
y \equiv 2^{-1} \times 2y \equiv 2^{-1} \times 74 \equiv 2^{-1} \times 2 \times 37 \equiv 37 \pmod{71}.
\]
Final answer: \( x \equiv -1 \pmod{71}, y \equiv 37 \pmod{71} \) Or, equivalently, \( x = 70 + 71n, y = 37 + 71m \) for \( n, m \in \mathbb{Z} \).

Alternatively, apply The Pulverizer to find the multiplicative inverse of 2 modulo 71. We need to find \( a, b \in \mathbb{Z} \) such that \( a \cdot 2 + b \cdot 71 = 1 \), so write:
\[
0 \cdot 2 + 1 \cdot 71 = 71
\]
\[
1 \cdot 2 + 0 \cdot 71 = 2
\]
\[
-35 \cdot 2 + 1 \cdot 71 = 1
\]
where we subtracted 35 times the 2nd equation from the 1st equation (here \( 35 = \lfloor 71/2 \rfloor \)). Therefore, \( 2^{-1} \equiv -35 \equiv 36 \pmod{71} \). Now multiply both sides of the equation \( 2y \equiv 3 \pmod{71} \) by 36 to get
\[
y \equiv 36 \cdot 2y \equiv 36 \cdot 3 \equiv 108 \equiv 37 \pmod{71}.
\]
Alternatively, apply the extended Euclidean algorithm to find the multiplicative inverse of 2 modulo 71, and then continue as above.

Alternatively, we could have started by isolating \( y \). We’d subtract 3 times the second equation from 2 times the first equation to get
\[
-2y \equiv -3 \pmod{71},
\]
continuing as before to calculate that \( y \equiv 37 \pmod{71} \). Then, we can plug this into one of two original equations to find that \( x \equiv -1 \pmod{71} \).

Alternatively, solve for \( x \) in the first equation to get
\[
x \equiv 3^{-1} \times -2y \equiv 24 \times -2y \equiv -48y \equiv 23y \pmod{71},
\]
where we had to compute the modular inverse of 3 modulo 71 (namely, 23) along the way. Now plug this expression for \( x \) into the second equation, yielding
\[
2 \cdot 23y + 2y \equiv 1 \pmod{71},
\]
i.e., \( 48y \equiv 1 \pmod{71} \). Now calculate the modular inverse of 48 modulo 71 to find the value of \( y \). Then we can plug the known value for \( y \) into one of the equations and solve for \( x \).