Question 1. short answers [14 MARKS]

Part (a) [2 MARKS]

Read the two statements:

$$(\forall n \in \mathbb{N}, P(n)) \Rightarrow (\forall m \in \mathbb{N}, Q(m))$$
$$\forall n \in \mathbb{N}, P(n) \Rightarrow Q(n)$$

Define predicates $P(n)$ and $Q(n)$ so that one of the two statements is true and the other is false. You may use the predicate definition format from the course notes, e.g. $P(n)$: "...", for $n \in \mathbb{N}$.

solution: Define:

$$P(n) : n \text{ is odd, for } n \in \mathbb{N}.$$
$$Q(n) : n \text{ is even, for } n \in \mathbb{N}.$$

Since not all natural numbers are odd, the hypothesis of the first statement is false, so the entire statement is true by vacuous truth. However, the existence of one or more odd (and hence not even!) natural numbers means at least one counter-example for the second statement exists.

Part (b) [2 MARKS]

Define $U = \{n : n \in \mathbb{N} \wedge 3 \mid n\}$ and $V = \{n : n \in \mathbb{N} \wedge n > 34 \wedge n < 45\}$. Show the set $V \setminus U$ by listing all its elements.

solution: The set of natural numbers greater than 34 and less than 45 that are not multiples of 3 are:

$$\{35, 37, 38, 40, 41, 43, 44\}$$

Part (c) [2 MARKS]

The floor function is define by $\lfloor x \rfloor$: "The largest integer $\leq x$," for $x \in \mathbb{R}$. Consider this statement:

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \lfloor xy \rfloor = \lfloor x \rfloor \times \lfloor y \rfloor$$

Is the statement true or false? Briefly explain why or why not.

solutions: The statement is true. Let $x = 0$ and the left-hand side becomes the floor of 0, while the right-hand side becomes 0 also.

Part (d) [2 MARKS]

Define set $D = \{d : d \text{ is a dog}\}$, predicate $F(d)$: "d is furry," where $d \in D$, and predicate $Y(d)$: "d is yappy," where $d \in D$. Express the English statement "No yappy dog is furry." as a sentence in predicate logic. Your predicate logic sentence must use predicates F and Y and must be quantified over set D.

solution: Every dog is not both yappy and furry:

$$\forall d \in D, \neg Y(d) \vee \neg F(d)$$

Part (e) [2 MARKS]

Suppose S is a non-empty subset of $\mathbb{N}$. Write a predicate logic sentence expressing the claim that 17 is the smallest number belonging to S.

solution: 17 is an element of S and there is no smaller element:

$$17 \in S \wedge \forall s \in \mathbb{N}, s \in S \Rightarrow s \geq 17$$

Part (f) [2 marks]

Write the **negation** of the predicate logic sentence:

$$(p \Leftrightarrow q) \Rightarrow r$$

...in predicate logic **without** using the operators $\Leftrightarrow$ or $\Rightarrow$

solution: The hypothesis says that p and q have the same truth value, and we conjoin that with the negation of the conclusion:

$$((p \wedge q) \vee (\neg p \wedge \neg q)) \wedge \neg r$$

Part (g) [2 marks]

Fill in the last column of the truth table below, where T stands for "true" and F stands for "false."

solution: All rows where the conclusion is true are marked T. All rows where the hypothesis is false are also marked T. The remaining two rows have a true hypothesis and false conclusion, so they are marked F.

p	q	r	$(p \Leftrightarrow q) \Rightarrow r$
T	T	T	T
T	T	F	F
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	F

Question 2. divisibility [9 marks]

Recall that for integers m and n, $m \mid n$ is defined as $\exists k \in \mathbb{Z}, km = n$. Consider the the statement:

$$\forall a, b, p, q \in \mathbb{Z}, 7 \mid (ap + bq) \Rightarrow 7 \mid p \wedge 7 \mid q$$

Part (a) [1 mark]

Write the predicate logic **converse** of the statement.

solution:

$$\forall a, b, p, q \in \mathbb{Z}, 7 \mid p \wedge 7 \mid q \Rightarrow 7 \mid (ap + bq)$$

Part (b) [1 mark]

Write the predicate logic **contrapositive** of the statement.

solution:

$$\forall a, b, p, q \in \mathbb{Z}, 7 \nmid p \vee 7 \nmid q \Rightarrow 7 \nmid (ap + bq)$$

Part (c) [1 mark]

Write the predicate logic **negation** of the statement.

solution:

$$\exists a, b, p, q \in \mathbb{Z}, 7 \mid (ap + bq) \wedge (7 \nmid p \vee 7 \nmid q)$$

Part (d) [3 MARKS]

Spoiler: the statement is **false**. However, write a **header** for a "proof" of the statement as though it were true. Introduce all variables and assumptions that would be required, including any variables needed to "unpack" the divisibility predicates. For example $7 \mid s$ could be unpacked as $\exists k \in \mathbb{N}, 7k = s$, and k could be introduced by "Let $k =$ ____." The last sentence of your header should begin "We want to show..." where "..." indicates what remains to be proved, in the style of our course notes.

solution: Let $a, b, p, q \in \mathbb{Z}$. Assume $7 \mid (ap + bq)$, that is $\exists k_1 \in \mathbb{Z}, 7k_1 = (ap + bq)$. Let $k_2 =$ ____ and $k_3 =$ ____. We want to show that $p = 7k_2$ and $q = 7k_3$.

Part (e) [3 MARKS]

Write a **header** and **body** for a disproof of the statement.

solution: We will prove the negation of the original statement:

$$\exists a, b, p, q \in \mathbb{Z}, 7 \mid (ap + bq) \wedge (7 \nmid p \vee 7 \nmid q)$$

header: Let $a = b = 1$, let $p = 3$, $q = 4$, and $k = 1$. We want to show that $7k = (ap + bq) \wedge (7 \nmid p \vee 7 \nmid q)$.

body: Substiting the given values for a, p, b, q, and k:

$$7k = 7 = (1(3) + 1(4)) = (ap + bq)$$

so $7 \mid (ap + bq)$. However $7 \nmid 3$ and $7 \nmid 4$, so $7 \nmid p \vee 7 \nmid q$. ∎

Question 3. modular arithmentic [6 MARKS]

Recall that for $a, b, n \in \mathbb{Z}$, with $n \neq 0$ we say a is congruent to b modulo n if and only if $n \mid a - b$. In this case we write $a \equiv b \pmod{n}$, or equivalently $a \equiv b \bmod n$.

Recall also Theorem 2.19(3), proved in Problem Set #1, that for all $a, b, c, d, n \in \mathbb{Z}$, with $n \neq 0$, if $a \equiv c \bmod n$ and $b \equiv d \bmod n$, then $ab \equiv cd \bmod n$.

You may use Theorem 2.19(3) one or more times to prove the statement:

$$\forall a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}, a_1 \equiv b_1 \bmod 5 \wedge a_2 \equiv b_2 \bmod 5 \wedge a_3 \equiv b_3 \bmod 5 \Rightarrow a_1a_2a_3 \equiv b_1b_2b_3 \bmod 5$$

Part (a) [3 MARKS]

Write a **header** for proving the statement. Introduce all variables and assumptions that would be required, including any variables needed to "unpack" the divisibility predicates. For example $5 \mid s$ could be unpacked as $\exists k \in \mathbb{N}, 5k = s$, and k could be introduced by "Let $k =$ ____." The last sentence of your header should begin "We want to show..." where "..." indicates what remains to be proved, in the style of our course notes.

solution: Although solutions are possible unpacking congruence and divisibility, it seems handier to use 2.19(3). For thoroughness we introduce variables for divisibility, but we don't end up using them (although some fine proofs might use them).

header: Let $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}$. Assume: $a_1 \equiv b_1 \bmod 5 \wedge a_2 \equiv b_2 \bmod 5 \wedge a_3 \equiv b_3 \bmod 5$. In other words, $\exists k_1 \in \mathbb{Z}, 5k_1 = a_1 - b_1$, $\exists k_2 \in \mathbb{Z}, 5k_2 = a_2 - b_2$, and $\exists k_3 \in \mathbb{Z}, 5k_3 = a_3 - b_3$. We want to show that $a_1a_2a_3 \equiv b_1b_2b_3 \bmod 5$.

Part (b) [3 MARKS]

Write the **body** for the proof of the statement.

solution:

$$\begin{aligned}
a_1 &\equiv b_1 \bmod 5 && \text{\# by assumption} \\
a_2 &\equiv b_2 \bmod 5 && \text{\# by assumption} \\
a_1 a_2 &\equiv b_1 b_2 \bmod 5 && \text{\# by 2.19(3)} \\
a_3 &\equiv b_3 \bmod 5 && \text{\# by assumption} \\
a_1 a_2 a_3 &\equiv b_1 b_2 b_3 \bmod 5 \quad \blacksquare && \text{\# by 2.19(3)}
\end{aligned}$$