MATH 243 – Mathematical Structures, section 2
Final Exam Solutions

I. A) Let p, q represent any propositions. Construct the truth table for the proposition

(p implies q) if and only if ((p and not$q$) implies$notp$)

Solution:

p	q	(p implies q)	if and only if	((p and not q)	implies	not p)
T	T	T	T	$((F)$	T	$F)$
T	F	F	T	$((T)$	F	$F)$
F	T	T	T	$((F)$	T	$T)$
F	F	T	T	$((F)$	T	$T)$

(The column lined lined up under the "and" of "if and only if" is the truth value of the whole proposition. Note this is the basis of one form of proof by contradiction!)

B) Give the contrapositive form of the statement "If the product of two integers x, y is even, then x is even or y is even."

Solution: "If x is not even (odd) and y is not even (odd), then the product of the two integers x, y is not even (odd)."

C) Give the converse of the statement in part B.

Solution: "If x is even or y is even, then the product x, y is even."

II. All parts of this question refer to the mapping $f : \mathbf{Z} \to \mathbf{Z}$ defined by

$$f(x) = \begin{cases} 6x & \text{if } x \text{ is even} \\ 2 - x & \text{if } x \text{ is odd} \end{cases}$$

A) Let $U = \{1, 2, 3, 4, 5\}$. What is $f(U) \cap \{x \in \mathbf{Z} : x > 0\}$?

Solution: Since $f(1) = 1$, $f(2) = 12$, $f(3) = -1$, $f(4) = 24$, $f(5) = -3$, we see

$$f(U) \cap \{x \in \mathbf{Z} : x > 0\} = \{1, 12, 24\}.$$

B) Let $V = 4\mathbf{Z}$. What is $f^{-1}(V)$ for this mapping?

Solution: Note that if x is odd, then $f(x) = 2 - x$ is also odd. On the other hand, if $x = 2k$ is even, then $f(x) = f(2k) = 6 \cdot 2k = 4 \cdot 3k \in 4\mathbf{Z}$. Hence $f^{-1}(V) = 2\mathbf{Z}$ (all even numbers).

III. Give a precise statement of the Division Algorithm in $\mathbf{Z}$ and prove the Existence and Uniqueness parts.

Solution: Let N and $n > 0$ be integers. There exist unique integers q, r such that $N = qn+r$ with $0 \leq r < n$.

Existence: Consider the set $S = \{N - kn \mid k \in \mathbf{Z}\}$. Then $S \cap (\mathbf{Z}^+ \cup \{0\}) \neq \emptyset$. (The reason here is that if $N > 0$, then we can just take $k = 0$ to get a positive element of S. On the other hand if $N \leq 0$, we just need to take k to be a negative integer with absolute value large enough that $-N < -kn$.) Now by the Well-Ordering property, $S \cap (\mathbf{Z}^+ \cup \{0\})$ contains a smallest element. Call this smallest element r, and write $r = N - qn$ (that is, $k = q$ for some particular integer q from the definition of the set S). This gives $N = qn + r$ as required and we only need to show $0 \leq r < n$. Now, $r \geq 0$ is automatic by the way r was produced (it's the smallest non-negative element of S). Suppose that $r \geq n$. Then in the set S we also have $N - (q + 1)n = N - qn - n = r - n \geq 0$ but $r - n < r$. This contradicts the choice of r as the smallest non-negative element in S. With this proof by contradiction, we have shown $r \leq n$. Hence both of the required conditions hold and the existence part of the proof is complete.

Uniqueness: If $N = q_1 n + r_1$ and also $N = q_2 n + r_2$, where r_1 and r_2 both satisfy the statement of the theorem but $r_1 \neq r_2$, then we can assume $r_1 > r_2$. Setting the two expressions for N equal, we have $q_1 n + r_1 = q_2 n + r_2$, so $(q_2 - q_1)n = r_1 - r_2$. Now $r_1 - r_2 > 0$ but also $r_1 - r_2 \leq r_1 < n$. Hence $r_1 - r_2$ is a multiple of n that lies strictly between 0 and n. But that is a clear contradiction. Hence $r_1 = r_2$, and hence $q_1 = q_2$ as well.

IV. A) Use the Euclidean Algorithm to find the integer $d = \gcd(753, 156)$ and express d in the form $d = 753m + 156n$ for some integers m, n

Solution: Applying the Euclidean Algorithm,

$$\begin{aligned} 753 &= 4 \cdot 156 + 129 \\ 156 &= 1 \cdot 129 + 27 \\ 129 &= 4 \cdot 27 + 21 \\ 27 &= 1 \cdot 21 + 6 \\ 21 &= 3 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Hence the last nonzero remainder $3 = \gcd(753, 156)$. Now we apply the Extended Eu-

clidean Algorithm to find m, n:

$$\begin{array}{rrr} & 1 & 0 \\ & 0 & 1 \\ 4 & 1 & -4 \\ 1 & -1 & 5 \\ 4 & 5 & -24 \\ 1 & -6 & 29 \\ 3 & 23 & -111 \end{array}$$

Hence $23 \cdot 753 + (-111) \cdot 156 = 3$.

B) Let a, b, c be integers. Prove that $\gcd(ab, c) = 1$ if and only if $gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

Solution: $\Rightarrow$: Suppose that $\gcd(ab, c) = 1$. Then we know this means there exist integers m, n such that $m \cdot (ab) + n \cdot c = 1$. But then by the commutative and associative laws for multiplication in $\mathbf{Z}$, this implies that $(mb) \cdot a + n \cdot c = 1$. Since mb is an integer, this implies $\gcd(a, c) = 1$ since $\gcd(a, c)$ is the smallest positive integer in the set of integer linear combinations $\{pa + qc : p, q \in \mathbf{Z}\}$. Similarly, $(ma) \cdot b + n \cdot c = 1$ and that implies $\gcd(b, c) = 1$.

$\Leftarrow$: If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$, then there exist integers m, n, p, q such that $ma+nc = 1$ and $pb + qc = 1$. Multiplying these equations together, we get $1 = (ma + nc)(pb + qc) = (mp)(ab) + (npb + mqa + nqc)c$. Since $mp, npb + mqa + nqc \in \mathbf{Z}$, this shows $\gcd(ab, c) = 1$.

V. Let $f : A \to B$ be a mapping and $U, V \subseteq A$. For each statement give a proof if the statement is true, or give a counterexample if the statement is false. (A complete counterexample consists of specific sets A, B, U, and V, a mapping f, and a justification of why these data contradict the statement.)

A) If f is injective and $f(U) \subseteq f(V)$, then $U \subseteq V$.

Solution: This statement is *true*. Proof: Let $x \in U$. Then $f(x) \in f(U)$ by definition. Since $f(U) \subseteq f(V)$, we also have $f(x) \in f(V)$, and so $f(x) = f(x')$ for some $x' \in V$. However, we also know that f is injective, so $x = x' \in V$, so $x \in V$. Since this holds for all $x \in U$, $U \subseteq V$.

B) If f is surjective and $f(U) \subseteq f(V)$, then $U \subseteq V$.

Solution: This statement is *false*. Here's a counterexample. Let $A = \{1, 2\}$, $U = \{1\}$, $V = \{2\}$, $B = \{b\}$, and let $f : A \to B$ be the mapping defined by $f(1) = f(2) = b$. We clearly have f is surjective and $f(U) \subseteq f(V)$ since both sets are $B = \{b\}$. However $U \cap V = \emptyset$, so we do not have $U \subseteq V$.

VI. All parts of this question refer to $R = \mathbf{Z}/30\mathbf{Z}$, in which the operations are addition and multiplication mod 30.

A) Construct the addition and multiplication tables for the subset $T = \{[0], [6], [12], [18], [24]\}$ in R.

Solution: The addition table is

	[0]	[6]	[12]	[18]	[24]
[0]	[0]	[6]	[12]	[18]	[24]
[6]	[6]	[12]	[18]	[24]	[0]
[12]	[12]	[18]	[24]	[0]	[6]
[18]	[18]	[24]	[0]	[6]	[12]
[24]	[24]	[0]	[6]	[12]	[18]

The multiplication table is

	[0]	[6]	[12]	[18]	[24]
[0]	[0]	[0]	[0]	[0]	[0]
[6]	[0]	[6]	[12]	[18]	[24]
[12]	[0]	[12]	[24]	[6]	[18]
[18]	[0]	[18]	[6]	[24]	[12]
[24]	[0]	[24]	[18]	[12]	[6]

B) Which elements of R have multiplicative inverses? Explain how you know. We have a multiplicative inverse for $[a]$ if and only if $\gcd(a, 30) = 1$. This is because having a b such that $[a][b] = [1]$ is equivalent to an equation $a \cdot b = 1 + k \cdot 30$ for some integer, and this can be rearranged to say $b \cdot a + (-k) \cdot 30 = 1$, which is equivalent to $\gcd(a, 30) = 1$. The classes that have inverses are:

$$[1], [7], [11], [13], [17], [19], [23], [29]$$

VII. A) Prove by mathematical induction that

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$$

for all natural numbers $n \geq 1$.

Solution: The base case is $n = 1$, and the formula says in that case

$$\frac{1}{1 \cdot 2} = \frac{1}{1+1}.$$

This is clearly true since both sides give $\frac{1}{2}$. Now for the induction step, assume that

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k\cdot(k+1)}=\frac{k}{k+1}$$

and consider

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{k\cdot(k+1)}+\frac{1}{(k+1)(k+2)}.$$

By the induction hypothesis, this equals

$$\frac{k}{k+1}+\frac{1}{(k+1)(k+2)}.$$

Putting these terms over a common denominator, we have

$$\frac{k(k+2)+1}{(k+1)(k+2)}=\frac{k^2+2k+1}{(k+1)(k+2)}=\frac{(k+1)^2}{(k+1)(k+2)}.$$

Canceling one power of $k+1$ between the numerator and denominator, we see this equals $\frac{k+1}{k+2}$, as desired. The formula is thus true for all $n\geq 1$ by induction.

B) What is the least upper bound

$$L=\sup\left(\left\{\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}:n\geq 1\right\}\right)?$$

(This is the same set of numbers as in part A.) Prove your assertion by showing that for every real $\epsilon>0$, there exist some n such that

$$L-\epsilon<\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}\leq L.$$

Solution: The least upper bound is $L=1$. This follows by considering the equality proved in part A. First, it is clear that $\frac{n}{n+1}\leq 1$ for all $n\in\mathbf{N}$, so $L=1$ is an upper bound. But we also see that for all $n\geq 1$,

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}=1-\frac{1}{n+1}.$$

For all $\epsilon>0$, there exist $n\in\mathbf{N}$ such that $\frac{1}{n+1}<\epsilon$ and that implies

$$1-\epsilon<1-\frac{1}{n+1}=\frac{n}{n+1}\leq 1.$$

This shows that the least upper bound is $L=1$.

C) What does your argument in part B say about the sequence

$$a_n=\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}?$$

Solution: It says the sequence converges to $L=1$.