INTRODUCTION TO PROOFS – SOLUTIONS

MATH 10010
(Paper Code MATH-10010J)

January 2019 1 hour 30 minutes

[B] means bookwork
[H] means a very similar question has been seen in lectures, homework or on online quizzes
[US] means unseen but straightforward
[UC] means unseen and challenging

Section A: Short Questions

A1. (2+2+4 marks)

(i) Negate the following statement:

$$p \in \mathbb{P} \Longrightarrow (d \in \mathbb{N} \text{ such that } d \mid p \Rightarrow d = 1 \vee d = p)$$

(ii) State the contrapositive of the following statement:

$$\forall\ a, b \in \mathbb{Z}, \gcd(a, b) = c \Longrightarrow \exists\ x, y \in \mathbb{Z} \text{ such that } a = cx \wedge b = cy$$

(iii) Let P and Q be statements. Using a truth table, show that $\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$.

Solutions:

(i) [H] $p \in \mathbb{P} \wedge d \in \mathbb{N}$ such that $d \mid p \wedge d \neq 1 \wedge d \neq p$

(ii) [H] $\forall\ a, b \in \mathbb{Z}, \forall\ x, y \in \mathbb{Z}, a \neq cx \vee b \neq cy \Longrightarrow \gcd(a, b) \neq c$

(iii) [H] We have the following truth table:

P	Q	P∧ Q	¬(P∧Q)	¬P	¬Q	¬P∨¬Q
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Since the columns for the statements $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are the same, we must have that $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are equivalent.

A2. (2+2+2+2 marks)

Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $f((m,n)) = (m+n, n)$, and define $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $g((m,n)) = (m-n, n)$.

(i) Let $(m,n) \in \mathbb{Z} \times \mathbb{Z}$. Determine $(g \circ f)((m,n))$.

(ii) Let $(m,n) \in \mathbb{Z} \times \mathbb{Z}$. Determine $(f \circ g)((m,n))$.

(iii) What can we conclude from (i) and (ii)? Justify your answer.

(iv) Let $V = \{(2n, 0) : n \in \mathbb{N}\}$. Find $g^{-1}[V]$.

Solutions:

(i) [H] We have that

$$(g \circ f)((m,n)) = g(f((m,n))) = g((m+n,n)) = (m+n-n, n) = (m,n).$$

(ii) [H] We have that

$$(f \circ g)((m,n)) = g(g((m,n))) = g((m-n,n)) = (m-n+n, n) = (m,n).$$

(iii) [B] By (i) and (ii), we have that $g \circ f$ and $f \circ g$ are the identity functions on $\mathbb{Z} \times \mathbb{Z}$. This means that f and g are inverses of each other.

(iv) [H] By (iii), we have that $g^{-1} = f$. Therefore, we have that

$$\begin{aligned} g^{-1}[V] = f[V] &= \{f((m,n)) : (m,n) \in V\} \\ &= \{f((2n,0)) : n \in \mathbb{N}\} \\ &= \{(2n,0) : n \in \mathbb{N}\} \\ &= V. \end{aligned}$$

A3. (4+2+2 marks)

(i) Find $x \in \mathbb{Z}$ such that $x \equiv 2 \pmod{10}$ and $x \equiv 3 \pmod{7}$.

(ii) Does 0 divide 0? Justify your answer.

(iii) Let p_1 and p_2 be distinct primes. Determine $\operatorname{lcm}(p_1, p_2)$. Justify your answer.

Solutions:

(i) [H] [We have that $\gcd(10,7) = 1$, so we can so we can use the Chinese Remainder Theorem to solve this question.] We have that

$$\begin{aligned} 10 &= 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0, \end{aligned}$$

so

$$\gcd(10,7) = 1 = 7 - 2 \cdot 3 = 7 - 2(10-7) = 3 \cdot 7 - 2 \cdot 10.$$

Hence, we set

$$x = 3 \cdot 7 \cdot 2 - 2 \cdot 10 \cdot 3 = 42 - 60 = -18.$$

Therefore, $x = -18$. [We double check that $x = -18$ indeed gives the right solution: We have $-18 \equiv 2 \pmod{10}$ and $-18 \equiv 3 \pmod{7}$.]

(ii) [US] We have that $0 = 0 \cdot x$ for any $x \in \mathbb{Z}$. Hence, 0 divides 0 by definition.

(iii) [B] First, we note that since p_1 and p_2 are primes, then p_1 and p_2 are positive integers. Further, since they are distinct primes, we have that $\gcd(p_1, p_2) = 1$. Then

$$\operatorname{lcm}(p_1, p_2) = \frac{|p_1 p_2|}{\gcd(p_1, p_2)} = |p_1 p_2| = p_1 p_2.$$

A4. (2+2+2+2 marks)

(i) Let A and B be sets. What is the Cartesian Product of A and B?

(ii) Let A be a set. What is the power set $\mathscr{P}(A)$ of A?

(iii) Let $A = \{\emptyset\}$ and $B = \{\pi\}$.

(a) Find $\mathscr{P}(A) \times \mathscr{P}(B)$.

(b) Define an equivalence relation $\sim$ on $\mathscr{P}(A)$ by $M \sim N$ if and only if $(M, N) \in \mathscr{P}(A) \times \mathscr{P}(A)$. Find $[\emptyset]_\sim$.

Solutions:

(i) [B] We have that $A \times B = \{(a, b) : a \in A, b \in B\}$.

(ii) [B] We have that the power set of A is given by $\mathscr{P}(A) = \{B : B \subseteq A\}$.

(iii) [US]

(a) We have that $\mathscr{P}(A) = \{\emptyset, \{\emptyset\}\}$ and $\mathscr{P}(B) = \{\emptyset, \{\pi\}\}$. Hence, we have that

$$\mathscr{P}(A) \times \mathscr{P}(B) = \{(\emptyset, \emptyset), (\emptyset, \{\pi\}), (\{\emptyset\}, \emptyset), (\{\emptyset\}, \{\pi\})\}.$$

(b) We have that

$$\begin{aligned} [\emptyset]_\sim &= \{C \in \mathscr{P}(A) : C \sim \emptyset\} \\ &= \{C \in \mathscr{P}(A) : (C, \emptyset) \in \mathscr{P}(A) \times \mathscr{P}(A)\} \\ &= \{\emptyset, \{\emptyset\}\} \\ &= \mathscr{P}(A). \end{aligned}$$

A5. (2+3+3 marks)

(i) State (without proof) which of the following sets have the same cardinality:

$$\mathbb{R}_+, \quad \mathbb{Q}, \quad \{0, 1\}, \quad \mathbb{N}, \quad (2, 3)$$

(ii) Let A and B be sets. Prove that if A and B are countable, then $|A| = |B|$.

(iii) Find a partition P of $\mathbb{N}$ such that $P = \{A, B, C\}$, where $|A| = |B| = |C|$. Justify your answer.

Solutions:

(i) [US] We have that $\mathbb{R}_+$ and $(2, 3)$ have the same cardinality [since they are both in bijection with $\mathbb{R}$], and we have that $\mathbb{Q}$ and $\mathbb{N}$ have the same cardinality [since they are both countable].

(ii) [H] Since both A and B are countable, then there exist bijections $f : A \to \mathbb{N}$ and $g : \mathbb{N} \to B$. Then $g \circ f : A \to B$ is bijective, so $|A| = |B|$.

(iii) [US] [There are many solutions to this question]
Let $A = 3\mathbb{N} = \{3, 6, 9, \ldots\}, B = 3\mathbb{N} - 1 = \{2, 5, 8, \ldots\}$ and $C = 3\mathbb{N} - 2 = \{1, 4, 7, \ldots\}$. Then $|A| = |B| = |C|$ and $A \cup B \cup C = \mathbb{N}$ but $A \cap B = A \cap C = B \cap C = \emptyset$. Hence, $P = \{A, B, C\}$ forms the required partition.

Section B: Longer Questions

B1. (i) (4+4+2 marks)
We define the *floor function* $f : \mathbb{R}_+ \to \mathbb{Z}$ by $f(x) = \lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\}$.

(a) Prove or disprove that f is injective.

(b) Prove or disprove that f is surjective.

(c) Is f bijective? Justify your answer.

(ii) (2+8 marks)

(a) Let $f : X \to Y$ and let $V \subseteq Y$. What is the definition of the inverse image of V under f?

(b) Let $f : X \to Y$ and let $U, V \subseteq Y$. Prove that $f^{-1}[U] \cap f^{-1}[V] = f^{-1}[U \cap V]$.

(iii) (10 marks)
Let R be an equivalence relation on a non-empty set X. Then the *inverse relation* of R is given by $R^{-1} = \{(a, b) : (b, a) \in R\}$. Prove that R^{-1} is an equivalence relation on X.

Solutions:

(i) [US]

(a) We will show that f is not injective.
Let $x = 1$ and $y = \frac{3}{2}$. Then $x, y \in \mathbb{R}_+$ and $x \neq y$, but

$$f(x) = f(1) = \lfloor 1 \rfloor = 1 = \left\lfloor \tfrac{3}{2} \right\rfloor = f\left(\tfrac{3}{2}\right) = f(y).$$

Therefore, f cannot be injective.

(b) We will show that f is surjective.
Take $y \in \mathbb{Z}$, and set $x = y$. Since $y \in \mathbb{Z}$, then $x \in \mathbb{Z}$, so $x \in \mathbb{R}$ [since $\mathbb{Z} \subseteq \mathbb{R}$.] Moreover, we have that

$$f(x) = f(y) = \lfloor y \rfloor = y$$

since $y \in \mathbb{Z}$. Hence, f is surjective.

(c) No, f is not bijective since it is not injective.

(ii) (a) [B] We have that $f^{-1}[V] = \{x \in X : f(x) \in V\}$.

(b) [H] We consider two cases:

(1) Suppose that at least one of the sets U, V is empty. Without loss of generality, suppose $U = \emptyset$. Then

$$f^{-1}[U] \cap f^{-1}[V] = \emptyset \cap f^{-1}[V] = \emptyset = f^{-1}[\emptyset] = f^{-1}[\emptyset \cap V] = f^{-1}[U \cap V].$$

(2) Suppose U, V are both non-empty. Then

$$\begin{aligned} x \in f^{-1}[U] \cap f^{-1}[V] &\iff x \in f^{-1}[U] \wedge x \in f^{-1}[V] \\ &\iff f(x) \in U \wedge f(x) \in V \\ &\iff f(x) \in U \cap V \\ &\iff x \in f^{-1}[U \cap V]. \end{aligned}$$

Hence, $x \in f^{-1}[U] \cap f^{-1}[V]$ if and only if $x \in f^{-1}[U \cap V]$, so $f^{-1}[U] \cap f^{-1}[V] = f^{-1}[U \cap V]$.

By (1) and (2), we have that $f^{-1}[U] \cap f^{-1}[V] = f^{-1}[U \cap V]$ for any sets $U, V \subseteq Y$.

(iii) [US] We note that since R is an equivalence relation, we have that R is reflexive, symmetric and transitive.

(I) Reflexivity: Take $a \in X$. Then $(a, a) \in R$ since R is reflexive. Then $(a, a) \in R^{-1}$. Hence, R^{-1} is reflexive.

(II) Symmetricity: Take $a, b \in X$ such that $(a, b) \in R^{-1}$. Then $(b, a) \in R$. Since R is symmetric, then $(a, b) \in R$. Hence, $(b, a) \in R^{-1}$. Therefore, R^{-1} is symmetric.

(III) Transitivity: Take $a, b, c \in R^{-1}$ such that $(a, b), (b, c) \in R^{-1}$. Then $(b, a), (c, b) \in R$. Since R is transitive, then $(c, a) \in R$. Hence, $(a, c) \in R^{-1}$. Therefore, R^{-1} is transitive.

Since R^{-1} is reflexive, symmetric and transitive, then R^{-1} is an equivalence relation.

B2. (i) (2+8 marks)

(a) Let A and B be sets. What does it mean for A and B to have the same cardinality?

(b) Let $f : X \to Y$ be injective, and let $A \subseteq X$ be a non-empty set. Show that $|A| = |f[A]|$.

(ii) (6+4 marks)

(a) Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f((m, n)) = 5^m 11^n$. Prove that f is injective.

(b) Let $\mathbb{P}$ be the set of all primes. Explain why $\bigcup_{p\in\mathbb{P}} p\mathbb{N} = \mathbb{N}\backslash\{1\}$.

(iii) (2+8 marks)

(a) Let P and Q be statements. State the truth table for $P \iff Q$.

(b) Let $a_1 = a_2 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for all $n \in \mathbb{N}$ with $n \geq 3$. Let $P(n)$ be the following statement:

$$3 \mid n \text{ if and only if } a_n \in 2\mathbb{N}.$$

Prove that $P(n)$ holds for all $n \in \mathbb{N}$.

Solutions:

(i) (a) [B] We have that A and B have the same cardinality if there exists a bijection $f : A \to B$.

(b) [H] Define $g : A \to f[A]$ by $g(a) = f(a)$. Then for any $a \in A$, we have that $g(a) = f(a) \in f[A]$. Hence, g is indeed a function from A to $f[A]$.
We will show that g is injective. So suppose $a, b \in A$ such that $g(a) = g(b)$. Then $f(a) = g(a) = g(b) = f(b)$ which holds if and only if $a = b$ since f is injective. It follows that g is injective.
Since the co-domain of g is equal to its range, we have that g is surjective by definition.
Since g is injective and surjective, it is bijective. It follows that $|A| = |f[A]|$.

(ii) (a) [H] Take $(m, n), (s, t) \in \mathbb{N} \times \mathbb{N}$ such that $f((m, n)) = f((s, t))$. Then $5^m 11^n = f((m, n)) = f((s, t)) = 5^s 11^t$ which holds if and only if $5^m 11^n = 5^s 11^t$. Since $m, n \in \mathbb{N}$, then $5^m 11^n \geq 2$, so $5^m 11^n$ has a unique prime factorisation by the Fundamental Theorem of Arithmetic. Since 5 and 11 are prime, then we must have that $m = s$ and $n = t$. Hence $(m, n) = (s, t)$. Therefore, f is injective.

(b) [UC] Let $n \in \mathbb{N}$ such that $n \geq 2$. Then n has a unique prime factorisation by the Fundamental Theorem of Arithmetic, so we can write $n = p_1 p_2 \cdots p_m$ for some primes $p_1 \leq p_2 \leq \cdots \leq p_m$ and some $m \in \mathbb{N}$. Then $n \in p_1\mathbb{N}$ since $p_2 \cdots p_m \in \mathbb{N}$, so $n \in \bigcup_{p\in\mathbb{P}} p\mathbb{N}$. But 1 does not have a prime factorisation, so there exists no $p \in \mathbb{P}$ such that $1 \in p\mathbb{N}$. Hence, $\bigcup_{p\in\mathbb{P}} p\mathbb{N} = \mathbb{N}\backslash\{1\}$.

(iii) (a) [B] We have the following truth table:

P	Q	P⇔ Q
T	T	T
T	F	F
F	T	F
F	F	T

(b) [UC] First, we note that by part (a), we have that $P(n)$ holds if and only if either

(I) both $3 \mid n$ and $a_n \in 2\mathbb{N}$, or

(II) both $3 \nmid n$ and $a_n \notin 2\mathbb{N}$.

We will give a proof by strong induction.

Let $n = 1$. Then $3 \nmid 1$ and $a_1 = 1 \notin 2\mathbb{N}$. Then $P(1)$ holds.
Let $n = 2$. Then $3 \nmid 2$ and $a_2 = 1 \notin 2\mathbb{N}$. Then $P(2)$ holds.
Let $n = 3$. Then $3 \mid 3$ and $a_3 = a_2 + a_1 = 1 + 1 = 2 \in 2\mathbb{N}$. Then $P(3)$ holds.

Now, let $k \in \mathbb{N}$ with $k \geq 3$ and suppose that $P(i)$ holds for all $i \in \mathbb{N}$ with $3 \leq i \leq k$. Then both $P(k)$ and $P(k-1)$ hold. We consider two cases:

(1) Suppose $3 \mid k+1$. Then $3 \nmid k$ and $3 \nmid k-1$, so $a_k, a_{k-1} \notin 2\mathbb{N}$ by assumption. Hence, $a_{k+1} = a_k + a_{k-1} \in 2\mathbb{N}$.

(2) Suppose $3 \nmid k+1$. Then either $3 \nmid k$ and $3 \mid k-1$ or $3 \mid k$ and $3 \nmid k-1$. Either way, we have that, by assumption, one and only one of the terms a_k or a_{k-1} is in $2\mathbb{N}$. Therefore, $a_{k+1} = a_k + a_{k-1} \notin 2\mathbb{N}$.

Summarising, we have that if $P(i)$ holds for all $i \in \mathbb{N}$ with $3 \leq i \leq k$, then $P(k+1)$ holds. Hence, by the Strong Principle of Mathematical Induction, we have that $P(n)$ holds for all $n \in \mathbb{N}$.

[Note that we do not necessarily need the base case $n = 3$ since, in the inductive step, we are only using the fact that $k + 1 \geq 3$.]