UNIVERSITY OF BRISTOL

Examination for the Degree of B.Sc. and M.Sci. (Level C/4)

FOUNDATIONS AND PROOF – SOLUTIONS

MATH 10004

(Paper Code MATH-10004J)

January 2018 1 hour 30 minutes

This paper contains two sections, Section A and Section B. Please use a separate answer booklet for each section.
*Section A contains **five** short questions. **ALL** answers will be used for assessment. This section is worth 40% of the marks for the paper.*
*Section B contains **two** longer questions. **ALL** answers will be used for assessment. This section is worth 60% of the marks for the paper.*

Calculators are **not** *permitted in this examination.*

On this examination, the marking scheme is indicative and is intended only as a guide to the relative weighting of the questions.

Do not turn over until instructed.

Section A: Short Questions

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

A1. (2+2+4 marks)

(i) Negate the following statement:

$$(\exists\, m \in \mathbb{Z} \text{ such that } |a_m| \geq 5) \wedge (\forall\, n \in \mathbb{N}, n > m \implies |a_n| < 5)$$

(ii) State the contrapositive of the following statement:

$$\forall\, a, b \in \mathbb{Z}, \exists\, m \in \mathbb{Z} \text{ such that } b = am \implies a \mid b$$

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

Solutions:

(i) [H] $(\forall\, m \in \mathbb{Z}, |a_m| < 5) \vee (\exists\, n \in \mathbb{N} \text{ such that } n > m \wedge |a_n| \geq 5)$

(ii) [H] $\forall\, a, b \in \mathbb{Z}, a \nmid b \implies \forall\, m \in \mathbb{Z}, b \neq am$

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

P	Q	P$\Leftrightarrow$ Q	P $\implies$ Q	Q $\implies$ P	(P $\implies$ Q)$\wedge$(Q $\implies$ P)
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

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

A2. (4+2+2 marks)

(i) Find $x \in \mathbb{Z}$ such that $x \equiv 2 \pmod 3$ and $x \equiv 4 \pmod 5$.

(ii) Find $x \in \mathbb{Z}$ (with $0 \leq x \leq 6$) such that $x \equiv 3^{42} \pmod 7$.

(iii) Let $x, y \in \mathbb{Z}$. We say that x and y have the same *parity* if either both x and y are odd or both x and y are even. We define a relation on $\mathbb{Z}$ by $x \sim y$ if x and y have the same parity. For $x \in \mathbb{Z}$, list (without proof) all distinct equivalence classes of x.

Solutions:

(i) [H] [We have that $\gcd(3,5) = 1$, so we can use the Chinese Remainder Theorem to solve this problem.] First, we need to find $s, t \in \mathbb{Z}$ such that $\gcd(3,5) = 3s + 5t$. We have

$$\begin{aligned} 5 &= 3 + 2 \\ 3 &= 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

so

$$\gcd(3,5) = 1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5$$

Then $s = 2$ and $t = -1$. Hence, we set

$$x = 2 \cdot 3 \cdot 4 + (-1) \cdot 5 \cdot 2 = 24 - 10 = 14.$$

Therefore, $x = 14$. [We double check that $x = 14$ indeed gives the right solution: We have $14 \equiv 2 \pmod 3$ and $14 \equiv 4 \pmod 5$.]

(ii) [H] We have that $3^2 \equiv 9 \equiv 2 \pmod 7$ and $2^3 \equiv 8 \equiv 1 \pmod 7$, so

$$3^6 \equiv (3^2)^3 \equiv 2^3 \equiv 1 \pmod 7.$$

Then

$$3^{42} \equiv (3^6)^7 \equiv 1^7 \equiv 1 \pmod 7.$$

Therefore, $x = 1$.

(iii) [US] We have two distinct equivalence classes:

$$\begin{aligned} [x]_\sim &= \{x \in \mathbb{Z} : x \text{ is odd}\} = \{x \in \mathbb{Z} : x = 2n + 1, \text{ for some } n \in \mathbb{Z}\} \\ [y]_\sim &= \{y \in \mathbb{Z} : y \text{ is even}\} = \{y \in \mathbb{Z} : y = 2n, \text{ for some } n \in \mathbb{Z}\} \end{aligned}$$

A3. (2+2+4 marks)

(i) Define the Cartesian Product of $\mathbb{N}$ and $\mathbb{Z}$.

(ii) (a) Give an example of a partition of $\mathbb{Q}$.

(b) Prove that the example found in (a) is indeed a partition.

Solutions:

(i) [B] We have that $\mathbb{N} \times \mathbb{Z} = \{(x, y) : x \in \mathbb{N}, y \in \mathbb{Z}\}$.

(ii) [US] [There are many solutions to this.] One example of a partition of $\mathbb{Q}$ is given by

$$P = \{\{1\}, \{x \in \mathbb{Q} : x \neq 1\}\}.$$

(iii) [US] [We need to show that the union of all partition pieces is equal to $\mathbb{Q}$ and that the pairwise intersection of distinct partition pieces is empty.] Let $P_1 = \{1\}$ and $P_2 = \{x \in \mathbb{Q} : x \neq 1\}$. Then $P_1 \cup P_2 = \mathbb{Q}$. Further, we have that $P_1 \cap P_2 = \emptyset$. Therefore, we have that P is a partition of $\mathbb{Q}$.

A4. (3+3+2 marks)

(i) Define $f = \{(x^3, x) : x \in \mathbb{R}\}$. Is f a function? Justify.

(ii) Define $g = \{(a, \alpha), (b, \delta), (a, \gamma), (c, \delta)\}$ where $a, b, c, \alpha, \delta, \gamma$ are all distinct. Is g a function? Justify.

(iii) Let $X = \{x \in \mathbb{R} : x = 2n + 1, \text{ for some } n \in \mathbb{N}\}$. Define $h : X \to \mathbb{R}$ by $h(x) = 2x$. List the domain, co-domain and range of h.

Solutions:

(i) [H] Let $x, y \in \mathbb{R}$ with $x \neq y$. Then $x^3 \neq y^3$, so for each x^3 there exists a distinct value $f(x^3) = x$ such that $(x^3, f(x^3)) \in f$. Therefore, f is a function.

(ii) [H] We have that $(a, \alpha) \in g$ and $(a, \gamma) \in g$. Therefore, $g(a)$ does not give a unique value for a, so g cannot be a function.

(iii) [H] The domain of h is X, the co-domain of h is $\mathbb{R}$, and the range of h is equal to

$$h(X) = \{h(x) : x \in X\} = \{2x : x \in X\} = \{2(2n + 1) : n \in \mathbb{N}\} = \{4n + 2 : n \in \mathbb{N}\}.$$

A5. (2+4+2 marks)

(i) Let A, B be sets. Define what it means for A and B to have the same cardinality.

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

(iii) State the Cantor-Schröder-Bernstein Theorem.

Solutions:

(i) [B] A set A has the same cardinality as a set B if there exists a bijection $f : A \to B$.

(ii) [H] Since $|B| = |A|$, there exists a bijection $f : B \to A$. Since A is countable, there exists a bijection $g : A \to \mathbb{N}$. Then $g \circ f : B \to \mathbb{N}$ is bijective, so B is countable.

(iii) [B] Let X and Y be sets. If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.

Section B: Longer Questions

B1. (i) (2+8 marks)

(a) Define what it means for p to be prime.

(b) Find all primes p such that $p + 4 = n^2$ for some $n \in \mathbb{N}$.

(ii) (2+8 marks)

(a) Let A and B be sets. What does it mean for A to be a subset of B?

(b) Let A, B, and C be sets. Prove that $A\backslash(B \cap C) = (A\backslash B) \cup (A\backslash C)$.

(iii) (4+4+2 marks)

Define $f : \mathbb{R}^+ \to \mathbb{R}^+$ by $f(x) = \frac{2}{|x|}$.

(a) Prove or disprove that f is injective.

(b) Prove or disprove that f is surjective.

(c) Is f bijective? Briefly justify.

Solutions:

(i) (a) [B] An integer $p > 1$ is prime if the only divisors of p are 1 and p.

(b) [H] We have that $p = n^2 - 4 = (n + 2)(n - 2)$. By the Fundamental Theorem of Arithmetic, the only possible factors of p [and therefore $(n+2)(n-2)$] are 1 and p, so we need to consider two cases:
First, we let $n+2 = p$. Then $n = p-2$, so $p = (n+2)(n-2) = p(p-4)$. Dividing by p, we get that $1 = p - 4$ which holds if and only if $p = 5$, which is prime.
Second, we let $n + 2 = 1$. Then $n = -1$, so $p = (n + 2)(n - 2) = 1(-3) = -3$, which is a contradiction since p is prime [so $p > 1$].
Therefore, if p is prime such that $p + 4 = n^2$ for some $n \in \mathbb{N}$, then $p = 5$.
On the other hand, if $p = 5$, then $p + 4 = 5 + 4 = 9 = 3^2 = n^2$, where $n = 3 \in \mathbb{N}$.
Therefore, p is prime with $p + 1 = n^2$ for some $n \in \mathbb{N}$ if and only if $p = 5$.

(ii) (a) [B] We have that $A \subseteq B$ if every element of A is an element of B.

(b) [H] We have that

$$\begin{aligned} x \in A\backslash(B \cap C) &\Leftrightarrow x \in A \wedge x \notin B \cap C \\ &\Leftrightarrow (x \in A) \wedge \neg(x \in B \cap C) \\ &\Leftrightarrow (x \in A) \wedge \neg(x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A) \wedge (x \notin B \vee x \notin C) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \\ &\Leftrightarrow x \in A\backslash B \vee x \in A\backslash C \\ &\Leftrightarrow x \in (A\backslash B) \cup (A\backslash C) \end{aligned}$$

Hence $x \in A\backslash(B \cap C)$ if and only if $x \in (A\backslash B) \cup (A\backslash C)$. Therefore, $A\backslash(B \cap C) = (A\backslash B) \cup (A\backslash C)$.

(iii) (a) [H] We will prove that f is injective. Take $x, y \in \mathbb{R}^+$ and suppose that $f(x) = f(y)$. Then $\frac{2}{|x|} = f(x) = f(y) = \frac{2}{|y|}$ which holds if and only if $|x| = |y|$. Since both $x, y > 0$ [since $x, y \in \mathbb{R}^+$], it follows that $x = y$. Therefore, f is injective.

(b) [H] We will prove that f is surjective. [Scratch work: For $y \in \mathbb{R}^+$, we set $y = f(x) = \frac{2}{|x|}$. Then $\frac{2}{y} = |x| = x$ since $y > 0$.] So let $y \in \mathbb{R}^+$ and set $x = \frac{2}{y}$. Then $x \in \mathbb{R}^+$ since $y \in \mathbb{R}^+$ and $y > 0$. Further, we have that

$$f(x) = f\left(\tfrac{2}{y}\right) = \frac{2}{\left|\frac{2}{y}\right|} = \frac{2|y|}{2} = |y| = y$$

since $y > 0$ [since $y \in \mathbb{R}^+$]. Hence, f is surjective.

(c) [H] We have that f is bijective since it is both injective and surjective.

B2. (i) (8+2 marks)

(a) Prove by induction that $2^n > n^2$ for all $n \in \mathbb{N}$ with $n \geq 5$.

(b) Find all $n \in \mathbb{N}$ such that $2^n < n^2$.

(ii) (3+3+3+1 marks)

Let $A, B \in \mathscr{P}(\mathbb{Z})$ (where $\mathscr{P}(\mathbb{Z})$ denotes the Power Set of $\mathbb{Z}$). Define a relation on $\mathscr{P}(\mathbb{Z})$ by $A \sim B$ if $A \cap B = \emptyset$.

(a) Prove or disprove that $\sim$ is reflexive.

(b) Prove or disprove that $\sim$ is symmetric.

(c) Prove or disprove that $\sim$ is transitive.

(d) Is $\sim$ an equivalence relation? Briefly justify.

(iii) (2+8 marks)

(a) Let $a, b \in \mathbb{Z}$. What is the relationship between $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$?

(b) Let $a, b, m, n \in \mathbb{N}$ with $a, b \geq 2$. Show that if $\gcd(a, b) = 1$, then $\operatorname{lcm}(a^n, b^m) = a^n b^m$.

Solutions:

(i) (a) [H] Let $P(n)$ be the following statement: $2^n > n^2$. We will prove by induction that $P(n)$ holds for all $n \in \mathbb{N}$ with $n \geq 5$.
First, let us consider $n = 5$. Then $2^n = 2^5 = 32 > 25 = 5^2 = n^2$. Therefore, $P(1)$ is a true statement.
Now, let $k \in \mathbb{N}$ with $k \geq 5$, and suppose that $P(k)$ is a true statement. Then $2^k > k^2$. We have

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k > 2k^2 && [\text{since } 2^k > k^2] \\ &= k^2 + k^2 = k^2 + k \cdot k \geq k^2 + 5k && [\text{since } k \geq 5] \\ &= k^2 + 2k + 3k > k^2 + 2k + 1 && [\text{since } 3k > 1 \text{ since } k \geq 5] \\ &= (k+1)^2, \end{aligned}$$

so if $P(k)$ is true, then $P(k+1)$ is true. By the Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers $n \geq 5$.

(b) [US] We know that $2^n > n^2$ for all $n \in \mathbb{N}$ with $n \geq 5$. It remains to check four cases:
For $n = 1$, we have that $2^1 > 1^2$. For $n = 2$, we have that $2^2 = 4 = 2^2$. For $n = 3$, we have $2^3 = 8 < 9 = 3^2$. For $n = 4$, we have $2^4 = 16 = 4^2$. Therefore, $2^n < n^2$ for $n = 3$.

(ii) [US]

(a) [There are many solutions to this. Any non-empty subset of $\mathbb{Z}$ will work as a counter example.] Let $A = \{1\}$. Then $A \in \mathscr{P}(\mathbb{Z})$ and $A \cap A = A = \{1\} \neq \emptyset$. So A is not reflexive.

(b) Let $A, B \in \mathscr{P}$ such that $A \sim B$. Then $A \cap B = \emptyset$. Hence, we must also have that $B \cap A = \emptyset$, so $B \sim A$. Therefore, $\sim$ is reflexive.

(c) [There are many solutions to this. Any subsets of $\mathbb{Z}$ such that $A \cap B = \emptyset, B \cap C = \emptyset$ but $A \cap C \neq \emptyset$ will work.] Let $A = \{1\}, B = \{2\}$ and $C = \{1, 3\}$. Then $A, B, C \in \mathscr{P}(\mathbb{Z})$ and $A \cap B = \emptyset$ and $B \cap C = \emptyset$, so $A \sim B$ and $B \sim C$. But $A \cap C = \{1\} \neq \emptyset$, so $A \not\sim C$. Therefore, $\sim$ is not transitive.

(d) No, $\sim$ is not an equivalence relation since it is neither reflexive or transitive.

(iii) (a) [B] For $a, b \in \mathbb{Z}$, we have that $\gcd(a, b)\ \mathrm{lcm}(a, b) = |ab|$.

(b) [UC] Since $a, b \geq 2$, then by the Fundamental Theorem of Arithmetic we can write $a = p_1 p_2 \cdots p_s$ for some primes $p_1 \leq p_2 \leq \cdots \leq p_s$ and $s \in \mathbb{N}$ and we can write $b = q_1 q_2 \cdots q_t$ for some primes $q_1 \leq q_2 \leq \cdots \leq q_t$ and $t \in \mathbb{N}$. Since $\gcd(a, b) = 1$, then $\gcd(p_i, q_j) = 1$ for all $i, j \in \mathbb{N}$ with $1 \leq i \leq s$ and $1 \leq j \leq t$. We will show that $\gcd(a^n, b^m) = 1$.
To the contrary, suppose that $\gcd(a^n, b^m) \neq 1$. Then $\gcd(a^n, b^m) \geq 2$, so there exists a prime p such that $p \mid a^n$ and $p \mid b^m$. Since $a^n = (p_1 p_2 \cdots p_s)^n = p_1^n p_2^n \cdots p_s^n$, it follows that $p \mid p_i^n$ for some i. Since both p and p_i are prime, we must have that $p = p_i$. Similarly, if $p \mid b^m$, then $p = q_j$ for some j. Hence, $p = p_i = q_j$ which is a contradiction since $\gcd(p_i, q_j) = 1$. Hence, we must have that $\gcd(a^n, b^m) = 1$.
It follows that

$$\mathrm{lcm}(a^n, b^m) = \frac{|a^n b^m|}{\gcd(a^n, b^m)} = |a^n b^m|.$$

Since $a, b \geq 2$, then $|a^n b^m| = a^n b^m$. Hence, $\mathrm{lcm}(a^n, b^m) = a^n b^m$.