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-10004)

January 2015 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.

B=Bookwork, **S**=Seen, **P**=Partially seen, **U**=Unseen

Remarks made in square brackets [such as these] are not necessary for a complete solution.

Section A: Short Questions

A1. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 5x + 1$.

(a) (2 marks) Show that f is injective.

(b) (2 marks) Show that f is surjective.

(c) (2+2 marks) Find a formula for f^{-1}, and demonstrate that $f^{-1} \circ f$ is the identity function on $\mathbb{R}$.

Solutions: (B)

(a) Suppose $x_1, x_2 \in \mathbb{R}$ so that $f(x_1) = f(x_2)$. Thus $5x_1 + 1 = 5x_2 + 1$, so $5x_1 = 5x_2$ and hence $x_1 = x_2$. Therefore f is injective.

(b) Take any $y \in \mathbb{R}$. [Want: $5x + 1 = y$, so we need $5x = y - 1$, $x = \frac{y-1}{5}$.] Take $x = \frac{y-1}{5}$. [So $x \in \mathbb{R}$.] Then

$$f(x) = 5 \cdot \frac{y-1}{5} + 1 = y - 1 + 1 = y.$$

Thus f is surjective.

(c) Claim: $f^{-1}(y) = \frac{y-1}{5}$. To prove this, take $x \in X$. Then

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = f^{-1}(5x + 1) = \frac{(5x+1) - 1}{5} = \frac{5x}{5} = x.$$

Hence $f^{-1} \circ f$ is the identity function on X.

A2. (a) (3 marks) Negate the following statement:

$$\exists M \in \mathbb{R} \text{ so that } \forall n \in \mathbb{Z}_+, |a_n| \leq M.$$

(b) (5 marks) Let P, Q be propositions. Use a truth table to prove that

$$\neg(P \implies Q) \iff (P \wedge \neg Q).$$

Solutions: (B)

(a)

$$\neg[\exists M \in \mathbb{R} \text{ so that } \forall n \in \mathbb{Z}_+, |a_n| \leq M]$$
$$\iff \forall M \in \mathbb{R}, \exists n \in \mathbb{Z}_+ \text{ so that } |a_n| > M.$$

(b)

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

Thus for any truth values of P and Q, the truth values of $\neg(P \implies Q)$ and $P \wedge \neg Q$ the same, so $\neg(P \implies Q)$ and $P \wedge \neg Q$ are equivalent.

A3. (a) (3 marks) List all the elements in the set $\{1,2\} \times \{3,4\}$.

(b) (3 marks) List all the partitions of the set $\{1,2,3\}$.

(c) (2 marks) For $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_+$, when is $a \equiv b \pmod{n}$?

Solutions: (B)

(a) $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$

(b) $\{\{1,2,3\}\}$, $\{\{1,2\}, \{3\}\}$, $\{\{1,3\}, \{2\}\}$, $\{\{2,3\}, \{1\}\}$, $\{\{1\}, \{2\}, \{3\}, \}$

(c) $a \equiv b \pmod{n}$ when n divides $a - b$.

A4. (a) (5 marks) Use Euclid's algorithm to find $\text{hcf}(76, 13)$, and integers s, t so that $76s + 13t = \text{hcf}(76, 13)$.

(b) (1 mark) Find $x \in \mathbb{Z}$ so that $x \equiv 2 \pmod{76}$ and $x \equiv 5 \pmod{13}$. (You may write x as a sum of products.)

(c) (2 marks) Find $x \in \mathbb{Z}$ so that $0 \le x < 7$ and $x \equiv 3^5 \pmod{7}$.

Solutions: (B)

(a)

$$\begin{aligned} 76 &= 13 \cdot 5 + 11 \\ 13 &= 11 \cdot 1 + 2 \\ 11 &= 2 \cdot 5 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

So $\text{hcf}(76, 13) = 1$.

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - (13 - 11) \cdot 5 \\ &= 11 \cdot 6 - 13 \cdot 5 \\ &= (76 - 13 \cdot 5) \cdot 6 - 13 \cdot 5 \\ &= 76 \cdot 6 - 13 \cdot 35. \end{aligned}$$

[So with $s = 6$ and $t - -35$, we have $1 = 76s + 13t$.]

(b) Take $x = 76 \cdot 6 \cdot 5 - 13 \cdot 35 \cdot 2$.

(c) $3^2 \equiv 9 \equiv 2 \pmod{7}$, so

$$3^5 \equiv 3^2 \cdot 3^2 \cdot 3 \equiv 2 \cdot 2 \cdot 3 \equiv 12 \equiv 5 \pmod{7}.$$

Thus $x = 5$.

A5. (a) (2 marks) Define what it means for sets A and B to have the same cardinality.

(b) (2 marks) Define what it means for a set C to be countable.

(c) (4 marks) Which of the following sets are countable?

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}; \ \mathbb{Q}; \ \mathbb{R}; \ \mathcal{P}(\mathbb{Z})$$

(where $\mathcal{P}(\mathbb{Z})$ denotes the power set of $\mathbb{Z}$).

Solutions: (B)

(a) A and B have the same cardinality if there is a bijection $f : A \to B$.

(b) C is countable if there is a bijections $g : \mathbb{Z}_+ \to C$. [Or: C is countable if C is infinite and there is an injection $h : C \to \mathbb{Z}_+$.]

(c) (i), (ii) are countable; (iii), (iv) are not.

Section B: Longer Questions

B1. (a) (8 marks) Let A, B, C be subsets of a set X. Prove that

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C).$$

(b) (4 marks) Define $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ by $f(m,n) = (m,0)$. Let $C = \{(m,0) :\ m \in \mathbb{Z}_+ \}$. Find $f^{-1}(C)$.

(c) (4 marks) Suppose $f : X \to Y$ and $U \subseteq X$. Show that $U \subseteq f^{-1}(f(U))$.

(d) (6 marks) Suppose $f : X \to Y$, $g : Y \to X$, and $g \circ f$ is the identity map on X. Also suppose g is injective. Show that $f \circ g$ is the identity map on Y.

(e) (8 marks) Use induction on n to show that for all $n \in \mathbb{Z}_+$

$$\sum_{i=1}^{n} (3i-2)^2 = \frac{n(6n^2-3n-1)}{2}.$$

Solutions:

(a) (S)

$$\begin{aligned} x \in A \setminus (B \cap C) &\iff x \in A \wedge x \notin (B \cap C) \\ &\iff x \in A \wedge (x \notin B \vee x \notin C) \\ &\iff (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \\ &\iff (x \in A \setminus B) \vee (x \in A \setminus C) \\ &\iff x \in (A \setminus B) \cup (A \setminus C). \end{aligned}$$

Therefore [the elements of $A \setminus (B \cap C)$ are exactly the elements of $(A \setminus B) \cup (A \setminus C)$, so] $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

(b) (P)

$$\begin{aligned} f^{-1}(C) &= \{(m,n) \in \mathbb{Z} \times \mathbb{Z} :\ f(m,n) \in C \} \\ &= \{(m,n) \in \mathbb{Z} \times \mathbb{Z} :\ (m,0) \in C \} \\ &= \{(m,n) \in \mathbb{Z} \times \mathbb{Z} :\ m \in \mathbb{Z}_+ \}. \end{aligned}$$

[So $f^{-1}(C) = \mathbb{Z}_+ \times \mathbb{Z}$.]

(c) (S) Take $x \in U$. We have $x \in f^{-1}(f(U))$ if and only if $f(x) \in f(U)$. Since $x \in U$, we have $f(x) \in f(U)$, and hence $x \in f^{-1}(f(U))$. [Since this holds for all $x \in U$, we have $U \subseteq f^{-1}(f(U))$.]

(d) (S) Take $y \in Y$. Then [using that $g \circ f$ is the identity map on X],

$$g \circ f \circ g(y) = g \circ f(g(y)) = g(y).$$

Also, $g \circ f \circ g(y) = g(f \circ g(y))$. [So $g(y) = g \circ f \circ g(y) = g(f \circ g(y))$.] Since g is injective, this means that $y = f \circ g(y)$. As y was chosen arbitrarily from Y, this shows that $f \circ g$ is the identity map on Y.

(e) (P) Let $P(n)$ be the proposition that $\sum_{i=1}^{n}(3i-2)^2 = \frac{n(6n^2-3n-1)}{2}$. We use induction on n to show that $P(n)$ holds for all $n \in \mathbb{Z}_+$.

[Base case] $\sum_{i=1}^{1}(3i-2)^2 = (3\cdot 1-2)^2 = \frac{1\cdot(6\cdot 1^2-3\cdot 1-1)}{2}$. Thus $P(1)$ holds.
[Induction step:] Suppose $k \geq 1$ and $P(k)$ holds. Then

$$\begin{aligned}\sum_{i=1}^{k+1}(3i-2)^2 &= (3(k+1)^2-2)^2 + \sum_{i=1}^{k}(3i-2)^2 \\ &= (3k+1)^2 + \frac{k(6k^2-3k-1)}{2} \\ &= \frac{2(9k^2+6k+1)+(6k^3-3k^2-k)}{2} \\ &= \frac{6k^3+15k^2+11k+2}{2}.\end{aligned}$$

On the other hand,

$$\begin{aligned}\frac{(k+1)(6(k+1)^2-3(k+1)-1)}{2} &= \frac{(k+1)(6(k^2+2k+1)-3k-3-1)}{2} \\ &= \frac{(k+1)(6k^2+9k+2)}{2} \\ &= \frac{(6k^3+9k^2+2k)+(6k^2+9k+2)}{2} \\ &= \frac{6k^3+15k^2+11k+2}{2}.\end{aligned}$$

[Hence $\sum_{i=1}^{k+1}(3i-2)^2 = \frac{(k+1)(6(k+1)^2-3(k+1)-1)}{2}$.] Thus $P(k) \implies P(k+1)$. So by the principle of mathematical induction $P(n)$ holds for all $n \in \mathbb{Z}_+$.

B2. (a) (4 marks) State the Fundamental Theorem of Arithmetic.

(b) (9 marks) Find all primes p so that for some $n \in \mathbb{Z}_+$, $3p+1 = n^2$. Justify your answer carefully.

(c) (6 marks) Suppose p is an odd prime with $p \neq 3$. Prove that either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.

(d) (4 marks) Let A, B be sets. Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

(e) (7 marks) Let X be a set and $\sim$ a relation on X. Let

$$N = \{x \in X :\ \neg(x \sim x)\ \},$$

$$B = \{b \in X :\ (\forall n \in N,\ b \sim n) \wedge (\forall n \notin N,\ \neg(b \sim n))\ \}.$$

Show that $B = \emptyset$.

Solutions:

(a) (B) Every integer n with $n > 1$ can be factored uniquely as a product of primes (up to reordering).

(b) (S) Suppose $n \in \mathbb{Z}_+$ and p is a prime so that $3p + 1 = n^2$. Thus $3p = (n-1)(n+1)$. By the Fundamental Theorem of Arithmetic, $n - 1$ must be $1, 3, p$, or $3p$.

Suppose $n - 1 = 1$: Then $n + 1 = 3$, and hence $3p = (n-1)(n+1) = 3$. This implies that $p = 1$, which is not prime. [So $n - 1$ cannot be 1.]

Suppose $n - 1 = 3$: Then $n + 1 = 5$, and hence $3p = 3 \cdot 5$. This implies that $p = 5$, which is prime.

Suppose $n - 1 = p$: Then $n + 1 = p + 2$, so $3p = p(p + 2)$. Thus $p + 2 = 3$, so $p = 1$, which is not prime. [So $n - 1$ cannot be p.]

Suppose $n - 1 = 3p$: Then $n + 1 = 3p + 2$, so $3p = 3p(3p + 2)$. Thus $3p + 2 = 1$, which is impossible, since $3p + 2 > 1$. [So $n - 1$ cannot be $3p$.]

Hence if $n \in \mathbb{Z}_+$ so that $3p + 1 = n^2$, then $p = 5$. [On the other hand, with $p = 5$, we have $3p + 1 = 16 = 4^2$. So the only prime p so that $3p + 1 = n^2$ for some $n \in \mathbb{Z}_+$ is $p = 5$.]

(c) (U) Take $r \in \mathbb{Z}$ so that $0 \leq r < 6$ and $p \equiv r \pmod 6$. So 6 divides $p - r$, meaning that $p - r = 6k$ for some $k \in \mathbb{Z}$, and hence $p = 6k + r$. If $r = 0, 2$, or 4, then $2 | 6k + r$, which is impossible since $p = 6k + r$ is odd. If $r = 3$ then $3 | 6k + r$, which means the prime p is divisible by 3; so if $r = 3$ then $p = 3$, contradiction our hypothesis that $p \neq 3$. [So we cannot have $r = 0, 2, 3, 4$.] So with p an odd prime, $p \neq 3$, we must have $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.

(d) (P) Suppose $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Thus either $X \in \mathcal{P}(A)$, meaning $X \subseteq A$, or $X \in \mathcal{P}(B)$, meaning $X \subseteq B$. In either case, $X \subseteq A \cup B$, and hence $X \in \mathcal{P}(A \cup B)$.

(e) (S) Suppose there is some $b \in B$. So either $b \in N$ or $b \notin N$. Suppose first that $b \in N$. Then $\neg(b \sim b)$ [by the definition of N and the supposition that $b \in N$]. But then $\neg(\forall n \in N,\ b \sim n)$ [since $b \in N$ and $\neg(b \sim b)$], which means that $b \notin B$, contradicting the assumption that $b \in B$. So suppose $b \notin N$. Then [by the definition of N] we must have $b \sim b$. But then $\neg(\forall n \notin N,\ \neg(b \sim n))$, contradicting the assumption that $b \in B$. Hence supposing that there is some $b \in B$ leads to a contradiction; thus $B = \emptyset$.