MH1300 Foundations of Mathematics – Solutions

Final Examination, Academic Year 2016/2017, Semester 1

November 8, 2025

Summary

This paper focuses on core topics in foundational mathematics: quantified statements and proof methods, parity and divisibility, induction, set-theoretic identities, functions and inverse images, relations and equivalence classes, and Cartesian products. Early questions emphasise correct handling of logical structure (negation, contrapositive, contradiction) and basic number-theoretic arguments via cases and the Quotient–Remainder Theorem. Middle questions test fluency with induction inequalities, floor/ceiling functions, subset relations, and properties of inverses of relations. Later questions integrate Euclidean algorithm computations with abstract reasoning about products of sets and biconditionals. Standard approaches (direct proofs, proofs by contradiction/contrapositive, case splits, induction, and element-chasing in sets and relations) are sufficient throughout, though some parts admit alternative viewpoints (e.g. via modular arithmetic or structural set identities).

Question 1 [15 marks]

Prove or disprove each of the following.

(a) $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, \forall z \in \mathbb{R}, xy \leq z^2$. [4 marks]

(b) Let x be an integer. If x^2 is not divisible by 4, then x is odd. [4 marks]

(c) Let x and y be integers. If $x + y$ is even and y is odd, then x is odd. [3 marks]

(d) There exists an odd integer M such that for all real numbers $r > M$, we have $\frac{1}{2r} < 0.01$. [4 marks]

Solution

(a) **True.**

Proof: Fix arbitrary $y \in \mathbb{R}$. Take $x = -y \in \mathbb{R}$.

Then we show $\forall z \in \mathbb{R}, xy \leq z^2$.

Let z be arbitrary. Then $z^2 \geq 0$.

But $xy = (-y)(y) = -y^2 \leq 0$.

Therefore, $xy \leq 0 \leq z^2$. $\square$

(b) **True.**

Proof by Contrapositive: Suppose x is not odd.

Then x is even. Let $x = 2k$ for some $k \in \mathbb{Z}$.

Then $x^2 = 4k^2$.

Since $k^2 \in \mathbb{Z}$, x^2 is divisible by 4.

Thus, if x^2 is not divisible by 4, x cannot be even, so x must be odd. $\square$

(c) **True.**

Proof by Contradiction: Suppose the statement is false. Then $x + y$ is even, y is odd, but x is even.

Let $x = 2k$ and $y = 2\ell + 1$ for some $k, \ell \in \mathbb{Z}$.

Then $x + y = 2k + 2\ell + 1 = 2(k + \ell) + 1$, which is odd.

This contradicts our assumption that $x + y$ is even.

Therefore, x must be odd. $\square$

(d) **True.**

Proof: Take $M = 51$. Then M is an odd positive integer.

We show $\forall r \in \mathbb{R}, r > M \implies \frac{1}{2r} < 0.01$.

Fix $r > M = 51$. Then $r > 51$, so $2r > 102$.

Therefore, $\frac{1}{2r} < \frac{1}{102} < 0.01$. $\square$

Mark Scheme:

(a) Correct choice of x depending on y (e.g. $x = -y$), explanation that $xy \leq 0$ and $z^2 \geq 0$, and conclusion $\forall z, xy \leq z^2$. [4]

(b) Clear contrapositive statement, representation of even x as $2k$, computation of $x^2 = 4k^2$, and link to divisibility by 4. [4]

(c) Proper contradiction setup using even/odd parametrisations, with $x = 2k$, $y = 2\ell + 1$, derivation that $x + y$ is odd, and explicit contradiction with the hypothesis. [3]

(d) Choice of an odd M (e.g. 51), correct inequality chain $r > 51 \Rightarrow 2r > 102 \Rightarrow \frac{1}{2r} < \frac{1}{102} < 0.01$, and correct universal quantifier handling. [4]

Question 2 [15 marks]

(a) Let n be a positive integer. Prove that $n(n^4 - 1)$ is divisible by 5. [5 marks]

(b) Let x and y be any real numbers such that $x + y = n$ where n is an integer. Prove that $\lceil x \rceil + \lfloor y \rfloor = n$.

Here, $\lceil x \rceil$ is the ceiling function and $\lfloor y \rfloor$ is the floor function. [5 marks]

(c) Prove the following or give a counterexample: $\forall x, y \in \mathbb{R}, \lceil xy \rceil = \lceil x \rceil \cdot \lceil y \rceil$. [5 marks]

Solution

(a) **Proof by Cases:**

Let n be a positive integer.

By the Quotient–Remainder Theorem,

$$n = 5k, \quad 5k+1, \quad 5k+2, \quad 5k+3 \text{ or } 5k+4.$$

Note that

$$n(n^4 - 1) = n(n^2+1)(n^2-1) = n(n-1)(n+1)(n^2+1).$$

If $n = 5k$, then n is divisible by 5.

If $n = 5k+1$, then $n-1$ is divisible by 5.

If $n = 5k+4$, then $n+1$ is divisible by 5.

We are left with $n = 5k+2$ and $n = 5k+3$.

<u>Case 1:</u> $n = 5k+2$.

$$n^2 + 1 = 25k^2 + 20k + 4 + 1 = 5(5k^2 + 4k + 1) \text{ is divisible by 5.}$$

<u>Case 2:</u> $n = 5k+3$.

$$n^2 + 1 = 25k^2 + 30k + 9 + 1 = 5(5k^2 + 6k + 2) \text{ is divisible by 5.}$$

In any case, at least one factor among n, $(n-1)$, $(n+1)$, or (n^2+1) is divisible by 5, so $n(n^2-1)(n^2+1)$ is divisible by 5.

Hence $n(n^4-1)$ is divisible by 5. □

(b) **Proof:**

Since $x + y = n$, we have $x = n - y$.

We need to show $\lceil x \rceil + \lfloor y \rfloor = n$, i.e. $\lceil n - y \rceil = n - \lfloor y \rfloor$.

Since $\lfloor y \rfloor \leq y$, we have

$$n - \lfloor y \rfloor \geq n - y.$$

But $y < \lfloor y \rfloor + 1$, so

$$n - y > n - \lfloor y \rfloor - 1.$$

Putting these together,

$$n - \lfloor y \rfloor - 1 < n - y \leq n - \lfloor y \rfloor.$$

By the definition of ceiling, this implies

$$\lceil n - y \rceil = n - \lfloor y \rfloor.$$

Therefore $\lceil x \rceil + \lfloor y \rfloor = n$. □

(c) **False.**

Counterexample: Take $x = 2$ and $y = \frac{1}{2}$.

Then $\lceil xy \rceil = \lceil 1 \rceil = 1$.

But

$$\lceil x \rceil \cdot \lceil y \rceil = \lceil 2 \rceil \cdot \lceil \tfrac{1}{2} \rceil = 2 \cdot 1 = 2.$$

Since $1 \neq 2$, the statement is false. □

Mark Scheme:

(a) Correct decomposition $n(n^4 - 1) = n(n^2 - 1)(n^2 + 1)$, case split modulo 5 via the Quotient–Remainder Theorem, and verification that in all cases a factor is divisible by 5. [5]

(b) Use of $x + y = n$, rewriting $x = n - y$, construction of inequalities involving $\lfloor y \rfloor$, and correct application of the ceiling definition to obtain $\lceil n - y \rceil = n - \lfloor y \rfloor$. [5]

(c) Clear statement of a concrete counterexample, computation of both sides $\lceil xy \rceil$ and $\lceil x \rceil \lceil y \rceil$, and explicit conclusion that they differ. [5]

Question 3 [10 marks]

Prove by mathematical induction that for every integer $n \geq 2$, $3^n > n^2$.

Solution

Let $P(n)$ be the statement $3^n > n^2$.

We first check small cases:

$$P(1): \quad 3^1 > 1^2 \iff 3 > 1 \quad \text{(true)},$$
$$P(2): \quad 3^2 > 2^2 \iff 9 > 4 \quad \text{(true)}.$$

Now assume $P(n)$ holds, i.e. assume $3^n > n^2$ for some $n \geq 2$.

Since $n \geq 2$, we have $n^2 \geq 2n$ and $n^2 > 1$. Hence

$$n^2 + n^2 > 2n + 1 \quad \Rightarrow \quad 2n^2 > 2n + 1$$

and so

$$3n^2 > n^2 + 2n + 1 = (n+1)^2.$$

Using the inductive hypothesis $3^n > n^2$, we get

$$3^{n+1} = 3 \cdot 3^n > 3 \cdot n^2 > (n+1)^2.$$

Thus $P(n+1)$ holds whenever $n \geq 2$.

Therefore, by mathematical induction, $3^n > n^2$ holds for all integers $n \geq 2$. $\square$

[MH1300 note: the official MI proof concludes here.]

$$\therefore \; P(1) \wedge \big(P(k) \Rightarrow P(k+1)\big) \Rightarrow \; P(n) \; \forall n \in \mathbb{N} \textit{ (by MI)} \; \square$$

Mark Scheme:

- Correct definition of $P(n)$ and verification of base cases (including $n = 2$). [2]
- Use of the inductive hypothesis $3^n > n^2$ and derivation of the inequality $3n^2 > (n+1)^2$ for $n \geq 2$. [4]
- Correct chaining $3^{n+1} = 3 \cdot 3^n > 3n^2 > (n+1)^2$, and a clear concluding statement that the inequality holds for all $n \geq 2$ by induction. [4]

Question 4 [15 marks]

(a) Prove that $\{4n \mid n \in \mathbb{Z}\} \subsetneq \{2n \mid n \in \mathbb{Z}\}$. [4 marks]

(b) Let n be a positive integer. Prove that n is even if and only if $7n+4$ is even. [4 marks]

(c) Recall that a number n is a perfect square if there is an integer k such that $k^2 = n$. Prove that if n is a perfect square, then $n+2$ is not a perfect square. [7 marks]

Solution

(a) **Proof:**

First, we show $\subseteq$: Let $x \in \{4n \mid n \in \mathbb{Z}\}$. Then $x = 4n$ for some $n \in \mathbb{Z}$, so $x = 2(2n)$ where $2n \in \mathbb{Z}$. Thus $x \in \{2n \mid n \in \mathbb{Z}\}$.

Now we show the inclusion is proper: Consider $2 \in \{2n \mid n \in \mathbb{Z}\}$ since $2 = 2 \cdot 1$. But if $2 = 4n$ for some $n \in \mathbb{Z}$, then $n = \frac{1}{2} \notin \mathbb{Z}$. Therefore, $2 \notin \{4n \mid n \in \mathbb{Z}\}$.

Hence, $\{4n \mid n \in \mathbb{Z}\} \subsetneq \{2n \mid n \in \mathbb{Z}\}$. □

(b) **Proof:**

Let n be a positive integer.

Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$.

Then, $7n + 4 = 7(2k) + 4 = 2(7k + 2)$ is even.

Now suppose n is odd. Then $n = 2m + 1$ for some $m \in \mathbb{Z}$.

So, $7n + 4 = 7(2m + 1) + 4 = 14m + 11 = 2(7m + 5) + 1$, which is odd.

Thus $7n + 4$ is even if and only if n is even. □

(c) **Proof by Contradiction:**

Assume n and $n + 2$ are both perfect squares. Let $n = k^2$ and $n + 2 = \ell^2$ for some positive integers k, ℓ.

Then $\ell^2 - k^2 = 2$, so $(\ell - k)(\ell + k) = 2$.

Since 2 is prime and $\ell + k > 0$, the only positive factorization of 2 is $2 = 1 \times 2$.

Thus, $\ell - k = 1$ and $\ell + k = 2$.

Adding these equations: $2\ell = 3$, so $\ell = \frac{3}{2} \notin \mathbb{Z}$.

This is a contradiction. Therefore, if n is a perfect square, then $n + 2$ is not a perfect square. □

Mark Scheme:

(a) Correct demonstration of inclusion $\{4n\} \subseteq \{2n\}$ and explicit example (e.g. 2) showing the inclusion is proper. [4]

(b) Both directions of the equivalence: even $n \Rightarrow 7n + 4$ even; odd $n \Rightarrow 7n + 4$ odd, using standard even/odd parametrisations. [4]

(c) Assumption that $n = k^2$ and $n+2 = \ell^2$, derivation $(\ell-k)(\ell+k) = 2$, analysis of factor pairs of 2, and contradiction via $\ell = \frac{3}{2} \notin \mathbb{Z}$. [7]

Question 5 [15 marks]

(a) Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be a function defined by $f(m, n) = m - n$.

  (i) Is f one-one? Justify your answer. [3 marks]

  (ii) Is f onto? Justify your answer. [3 marks]

(b) Let f be a function from A to B and let $D \subseteq A$ and $E \subseteq B$. Prove each of the following.

  (i) $f^{-1}(B - E) \subseteq A - f^{-1}(E)$. [4 marks]

  (ii) If f is a bijection and $f(D) = E$, prove that $f^{-1}(E) = D$. [5 marks]

Solution

(a) (i) **Not one-one.** Let $(1, 1) \neq (2, 2)$, but $f(1, 1) = 1 - 1 = 0 = 2 - 2 = f(2, 2)$.
Therefore, f is not injective.

(ii) **Is f onto? Yes.** For any $y \in \mathbb{Z}$, $f(y, 0) = y - 0 = y$.
Therefore, f is surjective.

(b) (i) **Proof:** Let $a \in f^{-1}(B - E)$. Then $f(a) \in B - E$.
Since $f(a) \in B$, we have $a \in A$. Since $f(a) \notin E$, by definition of the inverse image, $a \notin f^{-1}(E)$.
Therefore, $a \in A - f^{-1}(E)$, so $f^{-1}(B - E) \subseteq A - f^{-1}(E)$. □

(ii) **Proof:** Suppose f is 1-1 and onto, and assume $f(D) = E$.
Let $x \in f^{-1}(E)$.
Then, $f(x) \in E$.
Since $E = f(D)$, we have $f(x) \in f(D)$.
So, $\exists y \in D$ such that $f(y) = f(x)$.
Since f is 1-1, we get $x = y$.
So, $x \in D$.
Hence, $f^{-1}(E) \subseteq D$.
Now take $x \in D$. Since $f(D) = E$, we have $f(x) \in E$.
So, $x \in f^{-1}(E)$.
Thus $D \subseteq f^{-1}(E)$. Hence, $D = f^{-1}(E)$. □

Mark Scheme:

(a)(i) Identification that f is not injective and provision of a concrete example of distinct pairs with the same image. [3]

(a)(ii) Argument that for any $y \in \mathbb{Z}$, one can choose $(m, n) = (y, 0)$ so that $f(m, n) = y$, establishing surjectivity. [3]

(b)(i) Correct unpacking of $f^{-1}(B - E)$, membership reasoning, and conclusion that such points cannot belong to $f^{-1}(E)$; hence they lie in $A - f^{-1}(E)$. [4]

(b)(ii) Two inclusions proof of $f^{-1}(E) = D$ using the bijectivity of f and the assumption $f(D) = E$, with explicit use of injectivity in one direction and image containment in the other. [5]

Question 6 [12 marks]

(a) Let R be a relation on a set A, and define $R^{-1} = \{(a, b) \mid (b, a) \in R\}$. Prove that if R is transitive, then R^{-1} is transitive. [5 marks]

(b) Let S be a relation on the set of integers larger than 1 defined by: $n\,S\,m$ if and only if the smallest prime number dividing n equals the smallest prime number dividing m. Prove that S is an equivalence relation, and describe the distinct equivalence classes of S. [7 marks]

Solution

(a) **Proof:**

Assume R is transitive. Let $(x, y), (y, z) \in R^{-1}$.

Then $(y, x), (z, y) \in R$ (by definition of inverse).

Since R is transitive and $(z, y), (y, x) \in R$, we have $(z, x) \in R$.

By definition of the inverse, this means $(x, z) \in R^{-1}$.

Therefore, R^{-1} is transitive. $\square$

(b) **Showing S is an Equivalence Relation:**

Reflexive: Let $n > 1$. Then, the smallest prime number dividing n is clearly equal to the smallest prime dividing n itself. So, $n\,S\,n$.

Symmetric: Suppose $n\,S\,m$. Then the smallest prime dividing n is the smallest prime dividing m. Clearly, the smallest prime dividing m equals the smallest prime dividing n, so $m\,S\,n$.

Transitive: Suppose $n\,S\,m$ and $m\,S\,k$.

Then the smallest prime dividing n equals the smallest prime dividing m, and this also equals the smallest prime factor of k.

So, $n\,S\,k$.

Equivalence Classes:

The distinct classes of S are

$$[p]_S \quad \text{where } p \text{ is a prime number.}$$

Then

$$[p]_S = \{n \in \mathbb{Z} \mid n > 1 \text{ and } p \text{ is the smallest prime factor of } n\}.$$

In other words, each equivalence class consists of all integers greater than 1 whose smallest prime divisor is a fixed prime p. $\square$

Mark Scheme:

(a) Correct use of the definition of R^{-1}, translation of transitivity of R to obtain $(z, x) \in R$, and final step showing $(x, z) \in R^{-1}$. [5]

(b) Separate verification of reflexivity, symmetry, and transitivity for S based on smallest prime divisors, and clear description of equivalence classes indexed by primes p with the form $\{n > 1 : \text{smallest prime factor of } n = p\}$. [7]

Question 7 [18 marks]

(a) Prove that for any sets A and B, $A = B$ if and only if $A - B = B - A$. [5 marks]

(b) Use the Euclidean algorithm to find the greatest common divisor of the pair 1529 and 14038. [5 marks]

(c) Prove that for any non-empty sets A and B, and any sets C and D, $A \times B \subseteq C \times D$ if and only if $A \subseteq C$ and $B \subseteq D$. [8 marks]

Solution

(a) **Proof of Biconditional:**

Suppose $A = B$. Then, $A - B = A - A = \emptyset$ and likewise $B - A = \emptyset$, so $A - B = B - A$.

Now suppose $A - B = B - A$.

If $A - B \neq \emptyset$, then let $x \in A - B$. Then $x \in A$ and $x \notin B$. But since $A - B = B - A$, we also have $x \in B - A$, so $x \in B$ and $x \notin A$. This is a contradiction.

Thus, $A - B = \emptyset$. Similarly, $B - A = \emptyset$.

Having $A - B = \emptyset$ means $A \subseteq B$, and $B - A = \emptyset$ means $B \subseteq A$.

Hence $A = B$. $\square$

(b) **Euclidean Algorithm:**

$$
\begin{aligned}
14038 &= 1529 \times 9 + 277, \\
1529 &= 277 \times 5 + 144, \\
277 &= 144 \times 1 + 133, \\
144 &= 133 \times 1 + 11, \\
133 &= 11 \times 12 + 1, \\
11 &= 1 \times 11 + 0.
\end{aligned}
$$

The last nonzero remainder is 1.

Therefore, $\boxed{\gcd(1529, 14038) = 1}$. $\square$

(c) **Proof of Biconditional:**

($\Rightarrow$) Suppose $A \subseteq C$ and $B \subseteq D$.

Let $(a, b) \in A \times B$. Then $a \in A$ and $b \in B$.

Since $A \subseteq C$ and $B \subseteq D$, we have $a \in C$ and $b \in D$.

Thus $(a, b) \in C \times D$, so $A \times B \subseteq C \times D$.

($\Leftarrow$) Now suppose $A \times B \subseteq C \times D$ with A and B non-empty.

Let $a \in A$. Since $B \neq \emptyset$, fix some $b_0 \in B$.

Then $(a, b_0) \in A \times B$, so $(a, b_0) \in C \times D$.

Hence $a \in C$. Thus $A \subseteq C$.

To show $B \subseteq D$, similarly use $A \neq \emptyset$:

Let $b \in B$. Since $A \neq \emptyset$, fix $a_0 \in A$.

Then $(a_0, b) \in A \times B$, so $(a_0, b) \in C \times D$.

Thus $b \in D$. Hence $B \subseteq D$.

Therefore, $A \subseteq C$ and $B \subseteq D$. $\square$

Mark Scheme:

(a) Forward direction $A = B \Rightarrow A - B = B - A$, and reverse direction using contradiction or empty-difference argument to deduce both $A \subseteq B$ and $B \subseteq A$. [5]

(b) Correct execution of the Euclidean algorithm, including all intermediate remainders, and identification of the last nonzero remainder as the gcd. [5]

(c) ($\Rightarrow$) Clear proof that $A \subseteq C$ and $B \subseteq D$ imply $A \times B \subseteq C \times D$. ($\Leftarrow$) Use of non-emptiness of A and B to construct pairs and deduce $A \subseteq C$ and $B \subseteq D$ from $A \times B \subseteq C \times D$. [8]