MH1300 Foundations of Mathematics – Solutions

Final Examination, Academic Year 2024/2025, Semester 1

Compiled and typeset by QRS from the original handwritten solution

November 24, 2025

Question 1

(a) Prove that for every integer n, if $n^4 - 1$ is not divisible by 5 then n is divisible by 5.

(b) Let a, b, d be integers with $d > 1$. Prove that if $a \equiv b \pmod{d}$ then $a^2 \equiv b^2 \pmod{d}$.

(c) Are the following pair of statements logically equivalent?

$$(p \to q) \to (p \wedge r) \quad \text{and} \quad p \wedge (q \to r)$$

Justify your answer.

Solution

(a) **Proof by Cases:**

Let n be an integer. Suppose that n is not divisible by 5. There is an integer q such that

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

Since n is not divisible by 5, the first case is not possible.

We look at

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

<u>**Case 1:**</u> $n = 5q + 1$.

$$n^4 - 1 = (n^2+1)(n+1)(5q+1-1) = 5q\,(n^2+1)(n+1).$$

<u>**Case 2:**</u> $n = 5q + 2$.

$$n^4 - 1 = ((5q+2)^2+1)(n+1)(n-1)$$

$$= (25q^2 + 20q + 4 + 1)(n+1)(n-1)$$

For academic reference only. This document is provided for educational purposes and does not constitute an official question paper, answer key, or any formally authorised academic material. Its content is not guaranteed to be complete or accurate.

$$= 5(5q^2 + 4q + 1)(n + 1)(n - 1).$$

Case 3: $n = 5q + 3$.

$$n^4 - 1 = ((5q + 3)^2 + 1)(n + 1)(n - 1)$$
$$= (25q^2 + 30q + 9 + 1)(n + 1)(n - 1)$$
$$= 5(5q^2 + 6q + 2)(n + 1)(n - 1).$$

Case 4: $n = 5q + 4$.

$$n^4 - 1 = (n^2 + 1)(5q + 4 + 1)(n - 1)$$
$$= 5(q + 1)(n^2 + 1)(n - 1).$$

In all cases, $n^4 - 1$ is divisible by 5.

(b) Let $a, b, d > 1$ be integers. Suppose that $a \equiv b \pmod{d}$. Then $d \mid (b - a)$. So there is some integer k such that

$$kd = b - a.$$

Then

$$kd(b + a) = (b - a)(b + a) = b^2 - a^2.$$

Therefore,

$$d \mid (b^2 - a^2).$$

Thus,

$$a^2 \equiv b^2 \pmod{d}.$$

□

(c) They are logically equivalent.

$$\begin{aligned}
(p \to q) \to (p \wedge r) &\equiv \neg(p \to q) \vee (p \wedge r) && \text{(conditional rule)}\\
&\equiv \neg(\neg p \vee q) \vee (p \wedge r) && \text{(conditional rule)}\\
&\equiv (\neg\neg p \wedge \neg q) \vee (p \wedge r) && \text{(De Morgan's Law)}\\
&\equiv (p \wedge \neg q) \vee (p \wedge r) && \text{(Double Negation)}\\
&\equiv p \wedge (\neg q \vee r) && \text{(Distributive Law)}\\
&\equiv p \wedge (q \to r) && \text{(conditional rule)}
\end{aligned}$$

Thus, the statements are logically equivalent. □

Unofficial — QRS@NTU — qrsntu.org

Question 2

(a) Determine if the following is true or false. Justify your answer.

There are distinct positive integers $nandm$ such that $\frac{1}{m} + \frac{1}{n}$ is an integer.

(b) Determine if the following is true or false. Justify your answer.

Let $a > 1$ be an integer. If $a$is a perfect square, then $\sqrt[3]{a}$ is irrational.

(c) Determine if the following is true or false. Justify your answer.

If D and E are finite sets such that E has at least one more element than D, then $\mathcal{P}(E)$ has at least two more elements than $\mathcal{P}(D)$. Here, $\mathcal{P}(X)$is the power set of X.

Solution

(a) Let n, m be distinct positive integers.

Then $n \geq 1$ and $m > 1$.

<u>Case 1: $n = 1$.</u> Then since $n \neq m$, we have $m \geq 2$.

Thus
$$\frac{1}{n} + \frac{1}{m} = \frac{1}{1} + \frac{1}{m} \leq 1 + \frac{1}{2} = \frac{3}{2}.$$

And since $\frac{1}{m} > 0$, we also have
$$\frac{1}{n} + \frac{1}{m} = 1 + \frac{1}{m} > 1.$$

Thus
$$1 < \frac{1}{n} + \frac{1}{m} < \frac{3}{2},$$
hence $\frac{1}{n} + \frac{1}{m}$ is not an integer.

<u>Case 2: $m = 1$:</u> Then we argue exactly same as Case 1.

<u>Case 3: $n = 2$:</u> If $m = 1$ then we apply Case 2. Since $n \neq m$, we have $m \neq 2$. So we assume $m \geq 3$.

Then we have
$$\frac{1}{n} + \frac{1}{m} = \frac{1}{2} + \frac{1}{m} \leq \frac{1}{2} + \frac{1}{3} = \frac{5}{6}.$$

So
$$0 < \frac{1}{n} + \frac{1}{m} \leq \frac{5}{6},$$
hence $\frac{1}{n} + \frac{1}{m}$ is not an integer.

<u>Case 4: $m = 2$:</u> We argue similar to Case 3.

<u>Case 5: $n \neq 1$ & $n \neq 2$ & $m \neq 1$ & $m \neq 2$:</u> Then $n \geq 3$ and $m \geq 3$. Thus
$$\frac{1}{n} + \frac{1}{m} \leq \frac{1}{3} + \frac{1}{3} = \frac{2}{3}.$$

Since
$$0 < \frac{1}{n} + \frac{1}{m} \leq \frac{2}{3},$$
hence $\frac{1}{n} + \frac{1}{m}$ is not an integer.

In all cases,
$$\frac{1}{n} + \frac{1}{m}$$
is not an integer.

(b) This is false. Take any number which is both a perfect square and a perfect cube larger than 1. Eg, $a = 64$.

Then a is a perfect square ($a = 8^2$) but
$$\sqrt[3]{a} = 4$$
is rational.

(c) This is false. Let $D = \phi$, and $E = \{0\}$ are both finite sets, and E has one more element than D.

However,
$$P(D) = \{\phi\}$$
and
$$P(E) = \{\phi, \{0\}\}$$
and $P(E)$ has only one more element than $P(D)$.

Unofficial — QRS@NTU — qrsntu.org

Question 3

(a) Use mathematical induction to prove that for every integer $n \geq 1$,
$\sum_{j=1}^{3n} j(j-1) = n(9n^2-1)$.

(b) Use mathematical induction to prove that for every integer $n \geq 1$, and every sequence of non-negative real numbers $x_1, x_2, \ldots, x_n$,

if $x_1 + x_2 + \cdots + x_n = 0$, then $x_1 = x_2 = \cdots = x_n = 0$.

Solution

(a) Let $P(n) : \displaystyle\sum_{j=1}^{3n} j(j-1) = n\big(9n^2-1\big)$.

Base case : $P(1)$

$$\begin{aligned} \text{LHS} = \quad \sum_{j=1}^{3} j(j-1) &= 1\cdot 0 + 2\cdot 1 + 3\cdot 2 \\ &= 0+2+6 \\ &= 8 \\ \text{RHS} = 1\cdot(9\cdot 1^2 - 1) &= 8 \end{aligned}$$

So $P(1)$ is true.

Now assume $P(k)$ is true, i.e.

$$\sum_{j=1}^{3k} j(j-1) = k\big(9k^2-1\big).$$

Check $P(k+1)$:

$$
\begin{aligned}
\sum_{j=1}^{3(k+1)} j(j-1) &= \sum_{j=1}^{3k+3} j(j-1) \\
&= \sum_{j=1}^{3k} j(j-1) + (3k+1)(3k) \\
&\quad + (3k+2)(3k+1) + (3k+3)(3k+2) \\
&= k(9k^2-1) + (3k+1)(3k) + (3k+2)\big[3k+1+3k+3\big] \\
&= k(3k+1)(3k-1) + (3k+1)(3k) + (3k+2)(6k+4) \\
&= k(3k+1)\big[3k-1+3\big] + 2(3k+2)^2 \\
&= k(3k+1)(3k+2) + 2(3k+2)^2 \\
&= (3k+2)\big[k(3k+1) + 2(3k+2)\big] \\
&= (3k+2)\big[3k^2 + k + 6k + 4\big] \\
&= (3k+2)\big[3k^2 + 7k + 4\big] \\
&= (3k+2)(k+1)(3k+4) \\
&= (k+1)\big[(3k+3+1)(3k+3-1)\big] \\
&= (k+1)\big[(3k+3)^2 - 1\big] \\
&= (k+1)\big[9(k+1)^2 - 1\big] = \text{RHS}.
\end{aligned}
$$

So $P(k+1)$ is true.

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

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

(b) Let $P(n)$: for every sequence $X_1, X_2, \ldots, X_n$ of non negative real numbers, if $X_1 + X_2 + \cdots + X_n = 0$ then $X_1 = X_2 = \cdots = X_n = 0$.

Base case : $P(1)$. We need to check every non negative real number X_1. If $X_1 = 0$ then $X_1 = 0$ is true.

Assume $P(k)$ is true, i.e. for every sequence $X_1, X_2, \ldots, X_k$ of non negative real numbers, if $X_1 + X_2 + \cdots + X_k = 0$ then $X_1 = X_2 = \cdots = X_k = 0$.

Note that $P(k)$ is a conditional statement!

Now verify $P(k+1)$. Fix a sequence $X_1, X_2, \ldots, X_k, X_{k+1}$ of non negative real numbers, and assume that

$$X_1 + X_2 + \cdots + X_k + X_{k+1} = 0.$$

Then

$$X_1 + X_2 + \cdots + X_k = -X_{k+1}.$$

Since $X_{k+1} \geq 0$, hence RHS ≤ 0.

Since $X_1 \geq 0, X_2 \geq 0, \ldots, X_k \geq 0$, hence LHS ≥ 0.

But LHS = RHS, therefore both sides must be 0.

So,

$$X_1 + X_2 + \cdots + X_k = -X_{k+1} = 0. \qquad (*)$$

From $P(k)$, we know/assumed $X_1 + X_2 + \cdots + X_k = 0 \Rightarrow X_1 = X_2 = \cdots = X_k = 0$.

We also know $X_1 + X_2 + \cdots + X_k = 0$ from $(*)$.

So therefore, we conclude $X_1 = X_2 = \cdots = X_k = 0$.

From $(*)$ we also know $-X_{k+1} = 0$, so $X_{k+1} = 0$.

Therefore, $X_1 = X_2 = \cdots = X_k = X_{k+1} = 0$.

We have shown that starting from $X_1 + X_2 + \cdots + X_k + X_{k+1} = 0$ we derived $X_1 = X_2 = \cdots = X_k = X_{k+1} = 0$.

So, $P(k+1)$ is true.

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

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

Unofficial — QRS@NTU — qrsntu.org

Question 4

(a) If X, Y are sets, prove that $P(X - Y) - \{\emptyset\} = P(X) - P(Y)$.

Give a counterexample to show that $P(X - Y) - \{\emptyset\} = P(X) - P(Y)$is false for some X and Y.

(b) Let$A$,B and C be sets. Prove that

$(A \cap (A - B)) \cup (A^c \cup B)^c = A - B$.

(c) Prove or disprove the following statements:

(i)For every real number x,$\lfloor -x \rfloor = -\lceil x \rceil$.

(ii)For every real number x,$\lfloor -x \rfloor = -\lfloor x \rfloor$.

Solution

(a) Let X and Y be sets.

Let $A \in \mathcal{P}(X - Y) - \{\emptyset\}$.

Thus, $A \in \mathcal{P}(X - Y)$ and $A \notin \{\emptyset\}$.

By definition of powerset, A is not an element of set $\{\emptyset\}$.

This means $A \subseteq X - Y$. So $A \neq \emptyset$.

Since $A \subseteq X - Y$ and $X - Y \subseteq X$

Thus $A \subseteq X$, and so $A \in \mathcal{P}(X)$.

Since $A \neq \emptyset$,

A has some element $a \in A$. Since $A \subseteq X - Y$, it means $a \in X$, and $a \notin Y$. So, $A \not\subseteq Y$, so $A \notin \mathcal{P}(Y)$.

We conclude $A \in \mathcal{P}(X) - \mathcal{P}(Y) = \text{RHS}$.

Counter example to $\mathcal{P}(X - Y) - \{\emptyset\} = \mathcal{P}(X) - \mathcal{P}(Y)$.

$Y = \{0\},\ X = \{0, 1\}$. Then $X - Y = \{1\}$.

$\text{LHS} = \{\emptyset, \{1\}\} - \{\emptyset\} = \{\{1\}\}$.

$\text{RHS} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\} - \{\emptyset\} = \{\{1\}, \{0\}\}$. not equal.

(b) Using set identities,

$$\begin{aligned}
(A \cap (A - B)) \cup (A^c \cup B)^c &= (A \cap (A \cap B^c)) \cup (A^c \cup B)^c && \text{[Set difference Law]} \\
&= (A \cap (A \cap B^c)) \cup ((A^c)^c \cap B^c) && \text{[De Morgan's Law]} \\
&= (A \cap (A \cap B^c)) \cup (A \cap B^c) && \text{[Double complement Law, Commutativ} \\
&= (A \cap B^c) \cup ((A \cap B^c) \cap A) && \text{[Commutative Law]} \\
&= A \cap B^c && \text{[Absorption Law]} \\
&= A - B && \text{[Set difference Law]}
\end{aligned}$$

(c) By trying out a few values of x, it's easy to see that (i) is true, (ii) is false.

(i) By definition of $\lfloor -x \rfloor$,

$$\lfloor -x \rfloor \leq -x < \lfloor -x \rfloor + 1.$$

By definition of $\lceil x \rceil$,

$$\lceil x \rceil - 1 < x \leq \lceil x \rceil.$$

Adding the inequalities gives

$$\lfloor -x \rfloor + \lceil x \rceil - 1 < 0 < \lfloor -x \rfloor + \lceil x \rceil + 1.$$

$\lfloor -x \rfloor + \lceil x \rceil < 1 \quad$ and $\quad \lfloor -x \rfloor + \lceil x \rceil \leq 0$ since it's an integer.

$\lfloor -x \rfloor + \lceil x \rceil > -1 \quad$ and $\quad \lfloor -x \rfloor + \lceil x \rceil \geq 0$ since it's an integer.

We conclude $\lfloor -x \rfloor + \lceil x \rceil = 0$.

$\lfloor -x \rfloor = -\lceil x \rceil$.

(ii) Take $x = \frac{1}{2}$,

$$\lfloor -x \rfloor = \left\lfloor -\tfrac{1}{2} \right\rfloor = -1, \qquad -\lfloor x \rfloor = -\left\lfloor \tfrac{1}{2} \right\rfloor = 0$$

not equal.

Unofficial — QRS@NTU — qrsntu.org

Question 5

(a) Let x and y be two real numbers such that $0 < x < y$. Prove that there are integers n and m such that $nx \leq m \leq ny$.

(b) Prove that if a is an odd integer then $a^3 - a$ is a multiple of 8.

(c) Use the Euclidean algorithm to find $\gcd(630, 96)$.

Solution

(a) Let $0 < x < y$. Let

$$n = \left\lceil \frac{1}{y-x} \right\rceil \quad \text{and} \quad m = \lfloor ny \rfloor.$$

Then n, m are integers.

By definition of $\left\lceil \frac{1}{y-x} \right\rceil$, we have

$$\frac{1}{y-x} \leq \left\lceil \frac{1}{y-x} \right\rceil = n.$$

So

$$1 \leq n(y-x) \quad \text{(inequality does not flip around as } y - x > 0\text{).}$$

Thus $nx + 1 \leq ny$.

By definition of $\lfloor ny \rfloor$, we have

$$m \leq ny < m + 1.$$

Thus $nx \leq ny - 1 < m$, and so

$$nx < m \leq ny.$$

$$nx \leq m \leq ny.$$

(b) Let a be an odd integer. Then $a = 2k + 1$ for some integer k. Then

$$\begin{aligned}
a^3 - a &= a(a^2 - 1) \\
&= (2k+1)\big((2k+1)^2 - 1\big) \\
&= (2k+1)(4k^2 + 4k + 1 - 1) \\
&= (2k+1)(4k^2 + 4k) \\
&= 8k^3 + 12k^2 + 4k \\
&= 4k(2k^2 + 3k + 1) \\
&= 4k(2k+1)(k+1) \\
&= 4k(k+1)(2k+1).
\end{aligned}$$

By a result in class, $k(k+1)$ is even. Let $k(k+1) = 2\ell$. So,

$$a^3 - a = 4(2\ell)(2k+1) = 8\ell(2k+1),$$

which is divisible by 8.

Alternatively, you can proceed by the following.

Let a be an odd integer. Then $a = 4k+1$ or $a = 4k+3$ for some integer k.

<u>Case 1: $a = 4k+1$.</u>

$$\begin{aligned} a^3 - a &= (4k+1)(16k^2 + 8k + 1 - 1) \\ &= (4k+1)(16k^2 + 8k) \\ &= 8(4k+1)(2k^2 + k). \end{aligned}$$

<u>Case 2: $a = 4k+3$.</u>

$$\begin{aligned} a^3 - a &= (4k+3)(16k^2 + 24k + 9 - 1) \\ &= (4k+3)(16k^2 + 24k + 8) \\ &= 8(4k+3)(2k^2 + 3k + 1). \end{aligned}$$

In either case, $a^3 - a$ is divisible by 8.

(c)

$$\begin{aligned} 630 &= 96 \times 6 + 54 \\ 96 &= 54 \times 1 + 42 \\ 54 &= 42 \times 1 + 12 \\ 42 &= 12 \times 3 + \boxed{6} \quad \rightarrow \quad \gcd(630, 96) = 6 \\ 12 &= 6 \times 2 + 0. \end{aligned}$$

Question 6

(a) Find all complex numbers z satisfying the equation $z^3 = 3(1+i)$.

(b) Let $g : \mathcal{P}(\mathbb{R}) \to \mathcal{P}(\mathbb{R}^2)$ be defined by $g(A) = A \times A$. Determine if g is one-to-one and if g is onto.Justify your answers.

Solution

(a)

$$z^3 = 3(1+i) = 3e^{i\frac{\pi}{4}}$$

$$\begin{aligned} z &= \sqrt[3]{18}\, e^{i\frac{\pi/4+2k\pi}{3}}, \qquad k = 0,1,2 \\ z &= 18^{1/6}e^{i\frac{\pi}{12}}, \quad 18^{1/6}e^{i\frac{9\pi}{12}}, \quad 18^{1/6}e^{i\frac{17\pi}{12}}. \end{aligned}$$

(b) Let $g : \mathcal{P}(\mathbb{R}) \to \mathcal{P}(\mathbb{R}^2)$,

$$g(A) = A \times A.$$

g is one-to-one: Suppose $g(A) = g(B)$.

$$A \times A = B \times B.$$

Show: $A = B$. For any x,

$$x \in A \iff (x,x) \in A \times A \iff (x,x) \in B \times B \iff x \in B.$$

So $A = B$.

g is not onto:

Take $C = \{(0,1)\} \in \mathcal{P}(\mathbb{R}^2)$.

If $g(A) = C$, then

$$A \times A = \{(0,1)\}$$

so $(0,1) \in A \times A$.

So $0 \in A$.

This means $(0,0) \in A \times A = g(A) = C$.

Contradiction.

Question 7

(a) State the definition of each of the following:

(i) A symmetric binary relation R on a set A.

(ii) A transitive binary relation R on a set A.

(b) The relation R on $\mathbb{R}^2$ is defined by $(a,b)R(x,y)$ if and only if $a < x$ or ($a = x$ and $b < y$).

(i) Is R reflexive?

(ii) Is R symmetric?

(iii) Is R transitive?

Justify your answers.

(c) Let $X = \mathbb{R}^2 - \{(0,0)\}$ and define the relation T on the set X by $(a,b)T(x,y)$ iff there is some real number $c \neq 0$ such that $ca = x$ and $cb = y$.

(i) Show that T is an equivalence relation on X.

(ii) Describe the equivalence class of $(1,2)$.

Solution

(a) (i) A symmetric binary relation R is a relation on a set A such that for all $x, y \in A$, if $(x,y) \in R$ then $(y,x) \in R$.

(ii) A transitive binary relation R is a relation on a set A such that for every $x, y, z \in A$, if $(x,y) \in R$ and $(y,z) \in R$ then $(x,z) \in R$.

(b) No it is not reflexive.

(i) $0 < 0$ is false, so $(0,0)\,R\,(0,0)$ is false.

(ii) No it is not symmetric. Take $(0,0)$ and $(1,0)$. Then $(0,0)\,R\,(1,0)$ is true as $0 < 1$, but $(1,0)\,R\,(0,0)$ is false because $1 < 0$ is false and $1 = 0$ is false.

(iii) Yes it is transitive. Fix (a,b), (x,y), (u,v) such that $(a,b)\,R\,(x,y)$ and $(x,y)\,R\,(u,v)$.

<u>Case 1:</u> $a < x$.

Then since $(x,y)\,R\,(u,v)$, we have $x \leq u$.

This means $a < x \leq u \Rightarrow a < u$. So $(a,b)\,R\,(u,v)$ is true.

<u>Case 2:</u> $x < u$.

Then since $(a,b)\,R\,(x,y)$, we have $a \leq x$.

So $a \leq x < u \Rightarrow a < u$.

So again, $(a,b)\,R\,(u,v)$ is true.

<u>Case 3:</u> $a = x$ and $x = u$.

Then since $(a,b)\,R\,(x,y)$, we have $b \leq y$.

Since $(x, y)\, R\, (u, v)$, we have $y \leq v$.

So we have $a = x = u$ and $b \leq y \leq v$.

Thus $(a, b)\, R\, (u, v)$ is true.

(c) T **is reflexive:**

$1 \cdot a = a$ and $1 \cdot b = b$. So $(a, b)\, T\, (a, b)$ true.

T **is symmetric.**

Suppose $(a, b)\, T\, (x, y)$. Let $c \neq 0$ such that $ca = x$ and $cb = y$.

Then $a = \frac{1}{c}x$ and $b = \frac{1}{c}y$, where $\frac{1}{c} \neq 0$.

So $(x, y)\, T\, (a, b)$ true.

T **is transitive.**

Suppose $(a, b)\, T\, (x, y)$ and $(x, y)\, T\, (u, v)$. Let $c \neq 0, d \neq 0$ such that $ca = x$, $cb = y$, $dx = u$, $dy = v$. Then $dca = dx = u$ and $dcb = dy = v$ (by zero product property). So $(a, b)\, T\, (u, v)$.

Equivalence class of $(1, 2)$: $(a, b) \in [(1, 2)] \Leftrightarrow \exists c \neq 0$ such that $c \cdot 1 = a$ and $c \cdot 2 = b$ $\Leftrightarrow (a, b) = (c, 2c)$ for some $c \neq 0$.

This is the line $y = 2x$ with $(0, 0)$ removed.

Unofficial — QRS@NTU