MH1300 Foundations of Mathematics – Solutions

Final Examination, Academic Year 2023/2024, Semester 1

Compiled and typeset by QRS from the original handwritten solution

November 25, 2025

Question 1

(a) Prove that there do not exist positive integers a, b such that $a^2 + a + 1 = b^2$.

(b) Let c be an integer. Prove that c is divisible by 3 if and only if c^2 is divisible by 3.

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

$$p \to (q \vee r) \quad \text{and} \quad \neg q \to (\neg p \vee r).$$

Justify your answer.

Solution

(a) Suppose there are positive integers a, b such that

$$a^2 + a + 1 = b^2.$$

Then

$$b^2 = a^2 + a + 1 \quad > \quad a^2$$
$$\Rightarrow \; b > a \quad \text{(as both } a, b \text{ are positive)}$$

Method 1:

$$\begin{aligned} b^2 &= a^2 + a + 1 \qquad \text{(completing the square)} \\ &= (a+1)^2 - a \\ \text{So,} \quad a &= (a+1)^2 - b^2 \\ &= (a+1+b)(a+1-b) \end{aligned}$$

Since $b > a$, so $a + 1 - b \leq 0$, and $a + 1 + b \geq 0$, which means the product above ≤ 0.

But $a \geq 0$ is a contradiction.

Method 2:

$$\begin{aligned} & b^2 = a^2 + a + 1 \\ \Rightarrow\ & b^2 - a^2 = a + 1 \\ \Rightarrow\ & (b+a)(b-a) = a + 1 \end{aligned}$$

Since $b + a > a + a = 2a$, and $b - a > 0$,

$$\frac{(b+a)(b-a)}{a+1} > \frac{2a}{a+1} \quad \Rightarrow \quad a + 1 > 2a \quad \Rightarrow \quad 1 > a$$

Contradiction.

(b) Let c be an integer.

Suppose c is divisible by 3. Let $k \in \mathbb{Z}$ be such that $c = 3k$. Then

$$c^2 = 3ck = 3(ck).$$

Since $ck \in \mathbb{Z}$, we conclude that $3 \mid c^2$.

Suppose c^2 is divisible by 3. By QRT, there are 3 cases:

$$c = 3k,\ 3k+1,\ 3k+2 \quad \text{for some } k \in \mathbb{Z}.$$

We suppose that c isn't divisible by 3. Then $c = 3k + 1$ or $c = 3k + 2$ for some $k \in \mathbb{Z}$. (Goal: to obtain a contradiction in each case.)

<u>Case 1: $c = 3k + 1$.</u>

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

So, c^2 is *not* divisible by 3, contradiction.

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

$$\begin{aligned} c^2 &= (3k+2)^2 = 9k^2 + 12k + 4 \\ &= 3(3k^2 + 4k + 1) + 1. \end{aligned}$$

So, c^2 is not divisible by 3, contradiction.

Therefore we conclude that c must be divisible by 3.

(c) We show they are logically equivalent:

$$\begin{aligned}
p \to (q \vee r) &\equiv \neg p \vee (q \vee r) && \text{(logical equivalence for conditional)} \\
&\equiv (\neg p \vee q) \vee r && \text{(associative law)} \\
&\equiv (q \vee \neg p) \vee r && \text{(commutative law)} \\
&\equiv q \vee (\neg p \vee r) && \text{(associative law)} \\
&\equiv (\neg\neg q) \vee (\neg p \vee r) && \text{(double negation)} \\
&\equiv \neg q \to (\neg p \vee r) && \text{(logical law for conditional)}
\end{aligned}$$

Truth table solution is also fine.

Question 2

(a) Determine whether the following statement is true or false, and justify your answer: There are positive real numbers x, y such that $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$.

(b) Determine whether the following statement is true or false, and justify your answer: For every rational number $p > 0$ there is an irrational number z such that $p > z > 0$.

(c) Determine whether the following statement is true or false, and justify your answer: If A, B and C are sets then $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cap C)$.

Solution

(a) False. We want to show that there are no positive real numbers x, y such that

$$\sqrt{x+y} = \sqrt{x} + \sqrt{y}.$$

Suppose there are such $x, y > 0$.

$$\begin{aligned}
\sqrt{x+y} &= \sqrt{x} + \sqrt{y} \\
(\sqrt{x+y})^2 &= (\sqrt{x} + \sqrt{y})^2 \\
x + y &= x + y + 2\sqrt{xy} \\
2\sqrt{xy} &= 0 \\
\sqrt{xy} &= 0 \\
xy &= 0 \\
&\Rightarrow x = 0 \text{ or } y = 0 \text{ (by Zero Product Property),}
\end{aligned}$$

contradiction.

(b) This is true. Fix a rational number $p > 0$.

Take $z = \frac{p}{\sqrt{2}}$. Why do we choose $z = \frac{p}{\sqrt{2}}$? Recall that $\sqrt{2} \approx 1.4$, so $\frac{1}{\sqrt{2}}$ is between 0 and 1.

$$\Rightarrow \ 0 < z < p$$

Now furthermore, z is irrational, because let's suppose it is rational. Let $p = \frac{a}{b}$ and $z = \frac{c}{d}$ for some integers a, b, c, d and $b \neq 0, d \neq 0$. We also know $c \neq 0$ since $z > 0$.

$$\frac{p}{\sqrt{2}} = z = \frac{c}{d} \ \Rightarrow \ \sqrt{2} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}.$$

Since $bc \neq 0$ (by Zero Product Property), $\sqrt{2}$ is rational, a contradiction.

(c) This is false, students need to write down sets A, B, C and check the equality fails.

E.g. $A = \{0, 2, 3\},\ B = \{0, 1\},\ C = \{2, 3\}$.

Then

$$\text{LHS} = (A - B) \cap (A - C) = \{2, 3\} \cap \{0, 3\} = \varnothing.$$

$$\text{RHS} = A - (B \cap C) = A - \{3\} = \{0, 2\}.$$

LHS $\neq$ RHS.

Alternatively, take $A = \mathbb{Z},\ B =$ set of even integers, $C =$ set of odd integers. Check LHS $\neq$ RHS.

Question 3

(a) Use mathematical induction or strong mathematical induction to prove that for every integer $n \geq 12$, there are non-negative integers c and d such that

$$n = 7c + 3d.$$

(b) Prove that for every non-negative integer n,

$$1 \cdot 3 \cdot 5 \cdot 7 \cdots (2n+1) = \frac{(2n+2)!}{(n+1)! \cdot 2^{n+1}}.$$

Solution

(a) Let $P(n)$ be the property "there are non negative integers c, d such that $n = 7c + 3d$".

Use strong MI, $a = 12, b = 14$.

Base case. Verify $P(12)$. We need to find $c, d \geq 0$ s.t.

$$12 = 7c + 3d.$$

Take $c = 0, d = 4$, then

$$7c + 3d = 0 + 12 = 12.$$

So $P(12)$ is true.

Verify $P(13)$: Take $c = 1, d = 2$. Then

$$7c + 3d = 7 + 6 = 13.$$

So $P(13)$ is true.

Verify $P(14)$: Take $c = 2, d = 0$. Then

$$7c + 3d = 14 + 0 = 14.$$

So $P(14)$ is true.

Inductive step: Now fix $K \geq b = 14$ and assume

$$P(i) \text{ true for all } 12 \leq i \leq K.$$

WTS: $P(K+1)$ is true. Take $i = K + 1 - 3 = K - 2 \geq 14 - 2 = 12$.

Since $P(i)$ is true (by IH), there are integers $c, d \geq 0$ such that

$$i = 7c + 3d.$$

Thus

$$K + 1 = i + 3 = (7c + 3d) + 3 = 7c + 3(d + 1).$$

So $P(K+1)$ is true, and hence $P(n)$ true for all $n \geq 12$.

(b) Let $P(n)$:

$$1 \cdot 3 \cdot 5 \cdot 7 \cdots (2n+1) = \frac{(2n+2)!}{(n+1)!\,2^{\,n+1}}.$$

Base case $P(0)$**:** LHS $= 1$. RHS $= \dfrac{(0+2)!}{1 \cdot 1 \cdot 2} = \dfrac{2!}{2} = 1$. $\therefore P(0)$ is true.

Inductive Step: Let $K \geq 0$ and assume $P(K)$ is true.

$$\text{Inductive Hyp:} \quad 1 \cdot 3 \cdot 5 \cdot \ldots (2K+1) = \frac{(2K+2)!}{(K+1)!\,2^{\,K+1}}.$$

Need to show $P(K+1)$:

$$1 \cdot 3 \cdot 5 \cdots (2K+1)(2K+3) = \frac{[2(K+1)+2]!}{(K+2)!\,2^{\,K+2}}.$$

Start from LHS of $P(K+1)$:

$$1 \cdot 3 \cdot 5 \cdots (2K+1)(2K+3) = \frac{(2K+2)!}{(K+1)!\,2^{\,K+1}}\,(2K+3)$$

Consider RHS of $P(K+1)$:

$$\begin{aligned} \frac{(2K+4)!}{(K+2)!\,2^{\,K+2}} &= \frac{(2K+2)!(2K+3)(2K+4)}{(K+1)!(K+2)\,2^{\,K+1}\,2} \\ &= \frac{(2K+2)!(2K+3)}{(K+1)!\,2^{\,K+1}}. \end{aligned}$$

Thus the expressions are equal.

So $P(K+1)$ is true, and $P(n)$ true for all $n \geq 0$.

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

$$\therefore\; P(0) \wedge \big(P(k) \Rightarrow P(k+1)\big) \Rightarrow P(n)\ \forall n \in \mathbb{N}\ \textit{(by MI)} \qquad \square$$

Question 4

(a) Let A, B, C be sets. If $A \times C = B \times C$ and $C \neq \emptyset$, prove that $A = B$. Explain what happens if $C = \emptyset$.

(b) Let D be the set $\{0, 1\}$. Write down all the elements of $D \times \mathcal{P}(D)$. Recall that $\mathcal{P}(D)$ is the power set of D.

(c) Prove that $\sqrt{2} + \sqrt{7}$ is irrational.

Solution

(a) Suppose $A \times C = B \times C$, and $C \neq \varnothing$. Since $C \neq \varnothing$, let $x \in C$.

$\underline{A \subseteq B}$: let $a \in A$. Then $(a, x) \in A \times C$. Since $A \times C = B \times C$, $(a, x) \in B \times C$. This means $a \in B$.

$\underline{B \subseteq A}$: let $b \in B$. Then $(b, x) \in B \times C = A \times C$. So, $b \in A$.

If $C = \varnothing$ then $A \times C = \varnothing$ and $B \times C = \varnothing$ for any sets A and B. So the property is false. For example, $A = \mathbb{Z}$ and $B = \mathbb{R}$, $C = \varnothing$. Then $A \times C = B \times C$ but $A \neq B$.

(b) Let $D = \{0, 1\}$. First write down $\mathcal{P}(D) = \{\varnothing, \{0\}, \{1\}, D\}$.

So,

$$D \times \mathcal{P}(D) = \Big\{(0, \varnothing),\ (0, \{0\}),\ (0, \{1\}),\ (0, D),\ (1, \varnothing),\ (1, \{0\}),\ (1, \{1\}),\ (1, D)\Big\}.$$

8 elements.

(c) This is similar to a tutorial problem where you showed $\sqrt{2} + \sqrt{3}$ is irrational.

Suppose $\sqrt{2} + \sqrt{7}$ is rational. Let a, b be integers such that

$$\sqrt{2} + \sqrt{7} = \frac{a}{b}, \quad b \neq 0.$$

Then

$$a = b(\sqrt{2} + \sqrt{7}),$$

so $a \neq 0$ as well.

$$\sqrt{7} = \frac{a}{b} - \sqrt{2}$$

$$7 = \left(\frac{a}{b} - \sqrt{2}\right)^2 = \frac{a^2}{b^2} - 2\frac{a}{b}\sqrt{2} + 2,$$

$$2\frac{a}{b}\sqrt{2} = \frac{a^2}{b^2} - 5,$$

$$\sqrt{2} = \frac{b}{2a}\left(\frac{a^2}{b^2} - 5\right) = \frac{a^2 - 5b^2}{2ab}.$$

Since $a \neq 0, b \neq 0$, so $2ab \neq 0$ (zero product property). So $\sqrt{2}$ is rational, Contradiction.

Question 5

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

  (i) A surjective function.

  (ii) A one-to-one function.

(b) Suppose that S is a relation on a set B. Define

$$\bar{S} = \{(x, y) \in B \times B \mid (x, y) \notin S\}.$$

For each of the following, state whether the assertion is true or false, and justify your answer.

  (i) If S is symmetric, must $\bar{S}$ be symmetric?

  (ii) If S is reflexive, must $\bar{S}$ be reflexive?

  (iii) If S is transitive, must $\bar{S}$ be transitive?

(c) Use the Euclidean algorithm to find the greatest common divisor of the pair 12345 and 67890.

Solution

(a) (i) A function $f : A \to B$ is *surjective* if for every $b \in B$ there is some $a \in A$ such that $f(a) = b$.

  (ii) A function $g : C \to D$ is *one-to-one* if

$$\forall a, b \in C \ \text{ if } g(a) = g(b) \Rightarrow a = b,$$

or equivalently,

$$\forall a, b \in C \ \text{ if } a \neq b \Rightarrow g(a) \neq g(b).$$

(b) (i) False. Let $B = \mathbb{Z}$, and S be the relation nSm iff $n = m$. Then S is reflexive as $n = n$ holds for all $n \in \mathbb{Z}$. $\bar{S}$ isn't reflexive as $0 \neq 0$ is false, $0 \in \mathbb{Z}$.

  (ii) Suppose S is symmetric. We show $\bar{S}$ is symmetric. Let $(x, y) \in \bar{S}$. Then $(x, y) \notin S$. If $(y, x) \in S$ then $(x, y) \in S$ (by the fact that S is symmetric). So, $(y, x) \notin S$. So, $(y, x) \in \bar{S}$.

  (iii) This is false. For example, let $B = \mathbb{Z}$, S be the "divide" relation, i.e. $nSm \Leftrightarrow n \mid m$. Then S is transitive (shown in lecture). But $\bar{S}$ is not. For example,

$$2\,\bar{S}\,5 \quad \text{and} \quad 5\,\bar{S}\,8 \quad \text{and} \quad 2S8.$$

(c)

$$\gcd(12345, 67890)$$

$$
\begin{aligned}
67890 &= 12345 \times 5 + 6165 \\
12345 &= 6165 \times 2 + 15 \\
6165 &= 15 \times 411 + 0
\end{aligned}
$$

So, $\gcd(12345, 67890) = 15$.

Question 6

(a) Find all complex numbers z satisfying the equation $z^5 + 32 = 0$.

(b) Write down three functions $f_0 : \mathbb{Z} \to \mathbb{Z}$, $f_1 : \mathbb{Z} \to \mathbb{Z}$ and $f_2 : \mathbb{Z} \to \mathbb{Z}$ such that:

(i) f_0 is one-to-one but not onto.

(ii) f_1 is onto but not one-to-one.

(iii) f_2 is neither one-to-one nor onto.

Justify your answers.

(c) Suppose that $g : A \to B$ is a function. Prove that if $C \subseteq B$ and $D \subseteq B$, then

$$g^{-1}(C \cup D) = g^{-1}(C) \cup g^{-1}(D).$$

Solution

(a)

$$z^5 + 32 = 0$$

$$\begin{aligned} z^5 &= -32 = 32e^{i\pi}, \\ z &= 2e^{i(\pi + 2k\pi)/5}, \quad k = 0, 1, 2, 3, 4. \end{aligned}$$

(Any equivalent explicit listing of the 5 distinct roots earns full marks.)

(b) There are many options:

(i) $f_0(n) = 2n$ is one to one:

$$\begin{aligned} f_0(n) &= f_0(m) \\ \Rightarrow\ 2n &= 2m \\ \Rightarrow\ n &= m \end{aligned}$$

not onto: There is no n s.t. $f_0(n) = 2n = 1$ since $n = \frac{1}{2} \notin \mathbb{Z}$.

(ii) $f_1(n) = \left\lfloor \frac{1}{2} n \right\rfloor$.

$f_1(n)$ not one to one:

$$\begin{gathered} f_1(0) = \lfloor 0 \rfloor = 0 \\ f_1(1) = \left\lfloor \tfrac{1}{2} \right\rfloor = 0 \\ f_1(0) = f_1(1) \text{ but } 0 \neq 1. \end{gathered}$$

$f_1(n)$ is onto: Given any $m \in \mathbb{Z}$.

$$f_1(2m) = \left\lfloor \tfrac{1}{2} \cdot 2m \right\rfloor = \lfloor m \rfloor = m.$$

(iii) $f_2(n) = |n|$. alternatively $f_2(n) = n^2$.

$f_2(n)$ not one-to-one:

$$f_2(-1) = |-1| = 1 = f_2(1)$$

$f_2(n)$ is not onto : there is no n such that

$$f_2(n) = |n| = -1$$

as $|n| \geq 0$.

(c) Suppose $g : A \to B$, $C, D \subseteq B$.

$$g^{-1}(C \cup D) \subseteq g^{-1}(C) \cup g^{-1}(D) :$$

Let $a \in g^{-1}(C \cup D)$. Then $g(a) \in C \cup D$.

- If $g(a) \in C$, then $a \in g^{-1}(C) \Rightarrow a \in g^{-1}(C) \cup g^{-1}(D)$.
- If $g(a) \in D$, then $a \in g^{-1}(D) \Rightarrow a \in g^{-1}(C) \cup g^{-1}(D)$.

$$g^{-1}(C) \cup g^{-1}(D) \subseteq g^{-1}(C \cup D) :$$

Let $a \in g^{-1}(C) \cup g^{-1}(D)$.

- If $a \in g^{-1}(C)$ then $g(a) \in C$. So $g(a) \in C \cup D$ and hence $a \in g^{-1}(C \cup D)$.
- If $a \in g^{-1}(D)$ then $g(a) \in D$. So $g(a) \in C \cup D$ and hence $a \in g^{-1}(C \cup D)$.

Question 7

(a) Let K be the set $\{8k \mid k \in \mathbb{Z}\}$. Define a relation R on $\mathbb{Z}$ by aRb if and only if $a-b \in K$, for every $a, b \in \mathbb{Z}$.

   (i) Show that R is an equivalence relation on $\mathbb{Z}$.

   (ii) Describe the equivalence classes of R.

(b) Let S be a relation on a non-empty set A. We say that S is *round* if for every $x, y, z \in A$, if xSy and ySz then zSx. Prove that S is an equivalence relation if and only if S is reflexive and round.

Solution

(a) (i) R is reflexive: given any $a \in \mathbb{Z}$,

$$a - a = 0 = 8 \cdot 0 \text{ so } a - a \in K.$$

Hence aRa.

(ii) R is symmetric. Suppose $(a, b) \in R$. Then $a - b \in K$ and so

$$a - b = 8m \text{ for some } m \in \mathbb{Z}.$$

$$b - a = -8m = 8(-m). \text{ So } b - a \in K$$

and $(b, a) \in R$.

(iii) R transitive. Suppose $(a, b) \in R$ and $(b, c) \in R$. Then $a - b \in K$ and $b - c \in K$. So

$$a - b = 8m \text{ and } b - c = 8p \text{ for some } m, p \in \mathbb{Z}.$$

$$\begin{aligned} a - c &= (a - b) + (b - c) = 8m + 8p \\ &= 8(m + p). \end{aligned}$$

So, $a - c \in K$, and $(a, c) \in R$.

Note aRb iff $a - b \in K$

$$\begin{aligned} &\text{iff } 8 \mid a - b \\ &\text{iff } a \equiv b \pmod 8. \end{aligned}$$

There are 8 equivalence classes,

$$[0],\ [1],\ \ldots,\ [7]$$

where

$$[i] = \{\, 8k + i \mid k \in \mathbb{Z} \,\},\ i = 0, 1, 2, \ldots, 7.$$

(b) Suppose S is an equivalence relation.

Then S is obviously reflexive.

To show S is round, let $x, y, z \in A$ and assume xSy and ySz hold.

Since S is transitive, xSz holds. Since S is symmetric, zSx holds.

Now assume that S is reflexive and round. To show S is an equivalence relation, we need to show S is symmetric and transitive.

Symmetric: Suppose $x, y \in A$ and assume xSy. Since S is reflexive, ySy holds. Since S is round, ySx holds.

Transitive: Suppose $x, y, z \in A$ and assume xSy and ySz hold. Since S is round, zSx holds. Since S is symmetric, xSz holds (from above)

So, S is an equivalence relation.