

# MH1300 AY20/21 Final Exam

## Solutions

**Q1(a)**

Let  $a$  and  $b$  be integers.

Need to prove  $(a+b)^2$  is odd iff

$a, b$  are of opposite parity.

First direction: Assume  $(a+b)^2$  is odd. And  $a, b$  are of the same parity. (we want to derive a contradiction)

Since  $a, b$  are of the same parity, either  $a, b$  are both even, or  $a, b$  are both odd.

Case 1:  $a, b$  are both odd. Then, there exist

integers  $k, \ell$  such that  $a = 2k+1$  and  $b = 2\ell+1$ .

$$\begin{aligned} \text{Then, } (a+b)^2 &= (2k+1 + 2\ell+1)^2 \\ &= (2k+2\ell+2)^2 \\ &= 2(2(k+\ell+1))^2 \end{aligned}$$

Since  $2(k+\ell+1) \in \mathbb{Z}$ , this mean that  $(a+b)^2$  is even, contradicting our hypothesis that it is odd.

Case 2 :  $a, b$  are both even. Then, there exist integers  $k', l'$  such that  $a = 2k'$  and  $b = 2l'$ .

So,  $(a+b)^2 = (2k' + 2l')^2$   
 $= 2(2(k'+l'))^2$

Since  $2(k'+l')^2 \in \mathbb{Z}$ , this means  $(a+b)^2$  is even, contradicting our hypothesis that it is odd.

In both cases, we conclude that

$(a+b)^2$  is odd  $\Rightarrow a, b$  of opposite parity is true.

Second direction: Assume  $a, b$  are of opposite parity.

Then, either  $a$  is even and  $b$  is odd, or  
 $a$  is odd and  $b$  is even.

Case 1:  $a$  even &  $b$  is odd: let  $n, m \in \mathbb{Z}$  such that

$$a = 2n \text{ and } b = 2m+1.$$

$$\begin{aligned} \text{Then, } (a+b)^2 &= (2n+2m+1)^2 \\ &= 4(n+m)^2 + 4(n+m) + 1 \end{aligned}$$

$$= 2(2(n+m)^2 + 2(n+m)) + 1$$

Since  $2(n+m)^2 + 2(n+m) \in \mathbb{Z}$ , this means that  $(a+b)^2$  is odd.

Case 2: a odd and b even: Similar to case 1.

In each case, we conclude  $(a+b)^2$  is odd.

So, a, b of opposite parity  $\Rightarrow (a+b)^2$  is odd  
is true.

---

Remarks on Q1(c): You can use the theorems  
we discuss in class like  
odd \* odd = odd  
odd \* even = even  
etc.

instead of working directly with the  
definition of even / odd.

---

Q1(b)

Let  $n$  be an odd integer.

By the Quotient Remainder Theorem to  $d=4$ ,

$n = 4k, 4k+1, 4k+2 \text{ or } 4k+3$  for some  $k \in \mathbb{Z}$ .

Since we've assumed that  $n$  is odd, we can only have  $n = 4k+1 \text{ or } 4k+3$ .

Case 1:  $n = 4k+1$ : Then,  $n^2 + 3 = 16k^2 + 8k + 1 + 3$   
 $= 4(4k^2 + 2k + 1)$

$$\begin{aligned} n^2 + 7 &= 16k^2 + 8k + 1 + 7 \\ &= 8(2k^2 + k + 1) \end{aligned}$$

So,  $(n^2 + 3)(n^2 + 7) = 32(4k^2 + 2k + 1)(2k^2 + k + 1)$

Hence,  $32 \mid (n^2 + 3)(n^2 + 7)$ .

Case 2:  $n = 4k+3$ : Then,  $n^2 + 3 = 16k^2 + 24k + 9 + 3$   
 $= 4(4k^2 + 6k + 3)$

$$n^2 + 7 = 16k^2 + 24k + 9 + 7$$

$$= 8(2k^2 + 3k + 2)$$

Hence,  $(n^2 + 3)(n^2 + 7) = 32(4k^2 + 6k + 3)(2k^2 + 3k + 2)$

So,  $32 \mid (n^2 + 3)(n^2 + 7)$ .

In both cases, we obtain  $(n^2 + 3)(n^2 + 7)$  is divisible by 32.

Remarks: We need to apply QRT to  $d=4$ . If you

merely write  $n=2k+1$  by applying the definition that  $n$  is odd, you will not be able to easily show that  $(n^2 + 3)(n^2 + 7)$  is div. by 32.

Q1(c)

Using truth table:

P	q	$p \rightarrow q$	$(p \rightarrow q) \leftrightarrow q$	$((p \rightarrow q) \leftrightarrow q) \rightarrow p$
T	T	T	T	T
T	F	F	T	T
F	T	T	T	F
F	F	T	F	T

Since the output column contains both 'T' and 'F' values, this statement form is neither a contradiction nor a tautology.

Q2(a) This statement is false. Suppose it is true,

let  $x$  be a non zero rational number and  
 $y$  be a non zero irrational number and

$$\frac{1}{x} + \frac{x}{y} = 1. \quad \text{Then, } (xy) \left( \frac{1}{x} + \frac{x}{y} \right) = xy$$

$$\text{And so } y + x^2 = xy$$

$$\text{So } (1-x)y = -x^2$$

Note that  $x \neq 1$ , because otherwise,  $\frac{1}{x} + \frac{x}{y} = 1$  mean  
 $\frac{1}{y} = 0$ , which is impossible.

$$\text{So, } 1-x \neq 0, \text{ which mean } y = \frac{-x^2}{1-x}.$$

However, if  $x$  is rational, and  $1-x \neq 0$ , we

Conclude  $\frac{-x^2}{1-x}$  is rational. Hence,  $y$  is rational,

O Contradiction.

**Q2b** This is false. For a counter example, we need to find three set,  $A, B, C$  such that  $(A-B) \cup (A-C) \neq A - (B \cup C)$ .

For example,  $A = \{0, 1\}$ ,  $B = \{0\}$ ,  $C = \{1\}$ .

$$\text{Then } (A-B) \cup (A-C) = \{1\} \cup \{0\} = \{0, 1\} \quad \text{not equal.}$$
$$\text{And } A - \{B \cup C\} = \{0, 1\} - \{0, 1\} = \emptyset.$$

**Q2c** This is true. Suppose not. Then, there are integers  $n$  and  $m$  such that  $3 \mid n$  and  $3 \nmid m$  and  $3 \mid n+m$ . Since  $3 \mid n$  and  $3 \mid n+m$ , by a lemma in Section 4.8 of the lecture notes, we conclude  $3 \mid (n+m)-n$  i.e.  $3 \mid m$ , a contradiction to the hypothesis.

Q3a

Let  $P(n)$  be the statement

$$1 \cdot 4 + 2 \cdot 7 + \dots + n(3n+1) = n(n+1)^2, \quad n \geq 1.$$

Base case:  $P(1)$  is the statement

$$1 \cdot 4 = 1 \cdot (1+1)^2$$

$$\text{But } 1 \cdot 4 = 4 \text{ and } 1 \cdot (1+1)^2 = 1 \cdot 2^2 = 4.$$

So  $P(1)$  is true.

Inductive step: Assume  $k \geq 1$  and  $P(k)$  is true.

i.e. assume  $1 \cdot 4 + 2 \cdot 7 + \dots + k(3k+1) = k(k+1)^2$ .

We want to show  $P(k+1)$  is true.

i.e. WTS  $1 \cdot 4 + 2 \cdot 7 + \dots + (k+1)(3(k+1)+1) = (k+1)(k+2)^2$ .

$$\begin{aligned}
& \text{So, } 1 \cdot 4 + 2 \cdot 7 + \dots + (k+1)(3(k+1)+1) \\
&= [1 \cdot 4 + 2 \cdot 7 + \dots + k(3k+1)] + (3(k+1)+1)(k+1) \\
&= (\text{By IH}) \quad k(k+1)^2 + (3(k+1)+1)(k+1) \\
&= (k+1)(k(k+1) + 3k + 4) \\
&= (k+1)(k^2 + 4k + 4) \\
&= (k+1)(k+2)^2 \quad \text{So, } P(k+1) \text{ is true.}
\end{aligned}$$

Q3b Let  $P(n)$  be the statement

$$6 \cdot 7^n - 2 \cdot 3^n \text{ is divisible by } 4, \quad n \geq 1.$$

Base case:  $6 \cdot 7 - 2 \cdot 3$  is div by 4.

$$\text{Then } 6 \cdot 7 - 2 \cdot 3 = 42 - 6 = 36, \text{ which is div by 4.}$$

So,  $P(1)$  is true.

Inductive step: Let  $k \geq 1$  and assume  $P(k)$ .

i.e. let  $M$  be such that  $M$  is an integer and

$$4M = 6 \cdot 7^k - 2 \cdot 3^k.$$

$$\begin{aligned} \text{Consider } 6 \cdot 7^{k+1} - 2 \cdot 3^{k+1} &= 42 \cdot 7^k - 6 \cdot 3^k \\ &= 6 \cdot 7^k + 36 \cdot 7^k - 2 \cdot 3^k - 4 \cdot 3^k \\ &= (6 \cdot 7^k - 2 \cdot 3^k) + 36 \cdot 7^k - 4 \cdot 3^k \\ &= (\text{By IH}) \quad 4M + 4(9 \cdot 7^k - 3^k) \\ &= 4(M + 9 \cdot 7^k - 3^k) \end{aligned}$$

Since  $M + 9 \cdot 7^k - 3^k \in \mathbb{Z}$ , this means

$6 \cdot 7^{k+1} - 2 \cdot 3^{k+1}$  is div by 4, hence,

$P(k+1)$  is true.

(Q 4(a))

Let  $r$  be a real number.

Case 1:  $r \geq 0$ : Then  $|r| = r$  (by definition of  $|r|$ ).  
and  $-r \leq 0$ . So,  $|-r| = -(-r)$  (by definition of  $|-r|$ )

Since  $r = -(-r)$ , So,

$$|r| = |-r|.$$

Case 2:  $r < 0$ : Then,  $|r| = -r$ .

Since  $-r > 0$ , so,  $|-r| = -r$ .

$$\text{Hence, } |r| = |-r| = -r.$$

In both cases,  $|r| = |-r|$ .

(Q 4(b))

Let  $a, b, c, d \in \mathbb{Z}$  such that  $d \neq 0$  and

$d \mid a$  and  $d \mid b$  and  $d \nmid c$ .

Assume that there are integers  $x$  and  $y$  such that  $ax + by = c$ .

Since  $d \mid a$  and  $d \mid b$ , by lemma in section 4.8,

$d \mid ax + by$ . Hence,  $d \mid c$ .

This contradicts our assumptions.

So, there cannot be integers  $x$  and  $y$

such that  $ax + by = c$ .

Q 4(c)

Let  $B, C$  be sets such that

$$B \cup C = B \cap C.$$

Then  $B = C$ .

Let  $x \in B$ . Then,  $x \in B \cup C$ . Since  $B \cup C = B \cap C$ ,

we have  $x \in B \cap C$ . So,  $x \in B$  and  $x \in C$ .

Hence,  $x \in C$ . This shows  $B \subseteq C$ .

Now let  $x \in C$ . Then,  $x \in C \cup B$ . Since  $C \cup B = B \cap C$ ,

we have  $x \in B \cap C$ . So,  $x \in B$  and  $x \in C$ .

Hence,  $x \in C$ . This shows  $C \subseteq B$ .

We conclude, by the element method, that

$B \subseteq C$  and  $C \subseteq B$ , hence,  $B = C$ .

Q 5(a) Let  $A = \{\emptyset, \{\emptyset\}\}$ .

Then,  $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, A\}$ .

$A \times \mathcal{P}(A) = \{( \emptyset, \emptyset ), (\emptyset, \{\emptyset\}), (\emptyset, \{\{\emptyset\}\}), (\emptyset, A), (\{\emptyset\}, \emptyset), (\{\emptyset\}, \{\emptyset\}), (\{\emptyset\}, \{\{\emptyset\}\}), (\{\emptyset\}, A)\}$ , altogether 8 elements.

Q 5(b) Let  $B = \{b_1, \dots, b_k\}$ .

Any equivalence relation on  $B$  needs to be reflexive,

i.e.  $(b_1, b_1), (b_2, b_2), \dots, (b_k, b_k) \in R$  for any equivalence relation  $R$  on  $B$ .

Let  $R = \{(b_1, b_1), \dots, (b_k, b_k)\}$ .

Then  $R$  is clearly reflexive

To see that  $R$  is symmetric,

take  $(b, b') \in R$

Then,  $b = b'$ , and so,  $(b', b) = (b, b') \in R$ .

To see that  $R$  is transitive,

take  $(b, b')$  and  $(b', b'')$  in  $R$ .

Then,  $b = b'$  and  $b' = b''$ .

So,  $(b, b'') = (b, b') \in R$ .

So,  $R$  is an equivalence relation on  $B$ .

Furthermore, any equivalence relation on  $B$  must have  $R$  as a subset of it., and so must have size at least  $k$ . Hence,  $R$  is the smallest equivalence relation on  $B$ .

The largest equivalence relation on  $B$  is  $B \times B$ , which is clearly reflexive, symmetric and transitive.

Any (equivalence) <sup>binary</sup> relation on  $B$  is a subset of  $B \times B$ .

Q5cc)

Suppose  $C$  is a set and  $R$  is a reflexive and transitive relation on  $C$ .

$R \subseteq R \circ R$ : let  $(x, y) \in R$ . Since  $R$  is reflexive,  $(x, x) \in R$ .

So,  $(x, y) \in R \circ R$ .

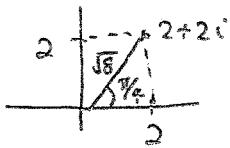
$R \circ R \subseteq R$ : let  $(x, y) \in R \circ R$ . Then  $(x, z) \in R$  and

$(z, y) \in R$  for some  $z \in C$ .

Since  $R$  is transitive,  $(x, y) \in R$ .

Q6(a)

$$z^3 - 2 - 2i = 0$$



$$z^3 = 2 + 2i$$

$$r = \sqrt{2^2 + 2^2} = 2\sqrt{2} \quad \theta = \tan^{-1} \frac{2}{2} = \frac{\pi}{4}$$

$$z^3 = 2\sqrt{2} e^{i\frac{\pi}{4}}$$

$$z = 8^{\frac{1}{6}} e^{i\Theta} \text{ where } \Theta = \frac{\pi}{12}, \frac{9\pi}{12}, \frac{17\pi}{12}$$

$$\text{i.e. } 8^{\frac{1}{6}} e^{i\frac{\pi}{12}}, 8^{\frac{1}{6}} e^{i\frac{3\pi}{4}}, 8^{\frac{1}{6}} e^{i\frac{17\pi}{12}}$$

Q6(b)

Let  $f: A \rightarrow B$ ,  $g: B \rightarrow C$ .

Suppose  $f, g$  are surjective.

Let  $z \in C$ . Since  $g$  is surjective, let  $y \in B$

such that  $g(y) = z$ . Since  $f$  is surjective,

let  $x \in A$  such that  $f(x) = y$ .

Since  $f(x) = y$  and  $g(y) = z$ , so

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

So,  $g \circ f$  is surjective.

Q6(c)

Suppose  $h: D \rightarrow E$ .

First direction: Suppose  $h$  is injective.

WTS: For any  $X \subseteq D$ ,  $h^{-1}(h(X)) = X$ . So, we fix such an  $X \subseteq D$ . [Recall:  $h(X) = \{h(b) \mid b \in X\}$   
 $h^{-1}(Y) = \{x \in D \mid h(x) \in Y\}$ ]

$h^{-1}(h(X)) \subseteq X$ : Let  $x \in h^{-1}(h(X))$ . By definition

of  $h^{-1}$ , there is some  $y \in h(X)$  such that  $h(x) = y$ . Since  $y \in h(X)$ , there is some  $a \in X$  such that  $h(a) = y$ . Since  $h$  is injective, and  $h(a) = y = h(x)$ , we have  $a = x$ .

So,  $x = a \in X$ .

$X \subseteq h^{-1}(h(X))$ : Let  $x \in X$ . Now by definition

of  $h(X)$ , we know  $h(x) \in h(X)$ .

Since  $h(x) \in h(X)$ , we conclude

$x \in h^{-1}(h(X))$ .

We conclude that  $h^{-1}(h(X)) = X$ .

Second direction: Suppose that for any  $X \subseteq D$ ,

$$h^{-1}(h(X)) = X.$$

WTS:  $h$  is injective. Fix  $p, q \in D$  such that

$$h(p) = h(q).$$

Let  $X = \{p\}$ . Then,  $X \subseteq D$  (since  $p \in D$ )

By assumption,  $h^{-1}(h(X)) = X$ .

However, note that since  $h(q) = h(p)$  and

$h(p) \in h(X)$ , so,  $h(q) \in h(X)$ , which

means that  $q \in h^{-1}(h(X))$ .

Since  $h^{-1}(h(X)) = X$ , so

$q \in X$ . Since  $X = \{p\}$  this means  $p = q$ .

[Q7(ai)] Let  $E, F$  be equivalence relations on  $A$ .

$E \cap F$  is reflexive: let  $a \in A$ . Then  $(a, a) \in E$  and  $(a, a) \in F$  since  $E, F$  are reflexive. So,  $(a, a) \in E \cap F$ .

$E \cap F$  is symmetric: let  $(a, b) \in E \cap F$ . Then  $(a, b) \in E$  and  $(a, b) \in F$ . Since  $E$  &  $F$  are symmetric, so  $(b, a) \in E$  and  $(b, a) \in F$ . So,  $(b, a) \in E \cap F$ .

$E \cap F$  is transitive: let  $(a, b) \in E \cap F$  and  $(b, c) \in E \cap F$ . Then  $(a, b) \in E$ ,  $(b, c) \in E$ ,  $(a, b) \in F$  and  $(b, c) \in F$ . Since  $E$  and  $F$  are transitive, so  $(a, c) \in E$  and  $(a, c) \in F$ . Hence,  $(a, c) \in E \cap F$ .

So,  $E \cap F$  is an equivalence relation on  $A$ .

(Q7a(ii))

Each equivalence class of ENF is of the form  $X \cap Y$  where  $X$  is an equivalence class of  $E$  and  $Y$  is an equivalence class of  $F$ ; and  $X \cap Y \neq \emptyset$ , and vice versa.

- $A/E_{\text{NF}} = \{ X \cap Y \mid X \in A/E \text{ and } Y \in A/F \text{ and } X \cap Y \neq \emptyset \}$
- For each  $a \in A$ ,  $[a]_{\text{ENF}} = [a]_E \cap [a]_F$

You can describe the equivalence classes of ENF in any of the ways above.

To prove it,

we let  $a \in A$  and WTS:  $[a]_{\text{ENF}} = [a]_E \cap [a]_F$ .

Let  $b \in [a]_{\text{ENF}}$ . Then  $(a, b) \in \text{ENF}$ , and  $(a, b) \in E$  and  $(a, b) \in F$ , so,  $b \in [a]_E \cap [a]_F$ .

Let  $b \in [a]_E \cap [a]_F$ . Then  $(a, b) \in E$  and  $(a, b) \in F$ . So,  $(a, b) \in \text{ENF}$  and so  $b \in [a]_{\text{ENF}}$ .

Q 7a(iii)

EUF is not necessarily transitive

(Although it has to be both reflexive and symmetric)

Take  $A = \{0, 1, 2\}$  and  $E$  to be  $\{(0,0), (1,1), (2,2), (0,1), (1,0)\}$   
and  $F$  to be  $\{(0,0), (1,1), (2,2), (1,2), (2,1)\}$ .

Then,  $E$  and  $F$  are clearly equivalence relations

on  $A$ . But  $EUF = \{(0,0), (1,1), (2,2), (1,2), (2,1), (0,1), (1,0)\}$

isn't transitive since  $(0,1) \in EUF$  and  
 $(1,2) \in EUF$  and  
 $(0,2) \notin EUF$

7b

$$198 = 168 \times 1 + 30$$

$$168 = 30 \times 5 + 18$$

$$30 = 18 \times 1 + 12$$

$$18 = 12 \times 1 + 6$$

$$12 = 6 \times 2$$



$$\gcd(168, 198) = 6.$$