Midterm Test Solutions

1. a) Find $\gcd(180, 42)$. [4 marks]

   b) Let $a, b, c \in \mathbb{Z}$ where $a \mid b$ and $b \mid c$. Prove that $a^2 \mid c^2$. [4 marks]

   c) Find $4^6 \ \% \ 13$. Using this result, or otherwise, find $4^{601} \ \% \ 13$. [2 marks]

Answer(s)

a) We apply the Euclidean algorithm as follows:

$$\begin{aligned}\gcd(180, 42) &= \gcd(12, 42) \\ &= \gcd(12, 6) \\ &= \gcd(0, 6) \\ &= 6.\end{aligned}$$

b) By the definition of $a \mid b$ and $b \mid c$, we have $b = ja$ and $c = kb$ for some integers j, k. We can substitute our expression of b into c to get $c = kja$. Squaring both sides, we get $c^2 = (kj)^2 a^2$. Since $(kj)^2$ is an integer, by definition, we have $a^2 \mid c^2$.

c) We can compute remainders for powers of 4 to get

$$\begin{aligned}4^1 \ \% \ 13 &= 4, \\ 4^2 \ \% \ 13 &= 3, \\ 4^3 \ \% \ 13 &= (3 \cdot 4) \ \% \ 13 = 12, \\ 4^4 \ \% \ 13 &= (12 \cdot 4) \ \% \ 13 = 9, \\ 4^5 \ \% \ 13 &= (9 \cdot 4) \ \% \ 13 = 10, \\ 4^6 \ \% \ 13 &= (10 \cdot 4) \ \% \ 13 = 1.\end{aligned}$$

We find that the remainders cycle every 6 powers so

$$4^{601} \ \% \ 13 = 4^{601 \ \% \ 6} \ \% \ 13 = 4^1 \ \% \ 13 = 4.$$

2. Let $U = \{x \in \mathbb{Z} : 0 \leq x \leq 10\}$ be the universal set. Define the following sets:

$$A = \{x \in U : x \text{ is prime}\}, \quad B = \{x \in U : |x| \leq 5\}, \quad C = \{x \in U : x \text{ is divisible by 3}\}.$$

   a) List the elements of U, A, B, C. [4 marks]

   b) Compute $(A \cap B) \cup C^c$. Show your steps. [3 marks]

   c) Compute $((A \cup B) \oplus C)$. Show your steps. [3 marks]

Answer(s)

a)
- Universal set: $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- Prime numbers in U: $A = \{2, 3, 5, 7\}$
- Numbers in U with absolute value ≤ 5: $B = \{0, 1, 2, 3, 4, 5\}$
- Numbers divisible by 3 in U: $C = \{0, 3, 6, 9\}$

b) To compute $(A \cap B) \cup C^c$, we find that

- Intersection of A and B: $A \cap B = \{2, 3, 5\}$
- Complement of C in U: $C^c = U \setminus C = \{1, 2, 4, 5, 7, 8, 10\}$
- Union of $(A \cap B)$ and C^c: $(A \cap B) \cup C^c = \{1, 2, 3, 4, 5, 7, 8, 10\}$

c) To compute $((A \cup B) \oplus C)$, we find that

- Union of A and B: $A \cup B = \{0, 1, 2, 3, 4, 5, 7\}$
- Symmetric difference between $(A \cup B)$ and C:

$$\begin{aligned}(A \cup B) \oplus C &= (A \cup B \setminus C) \cup (C \setminus A \cup B) \\ &= \{1, 2, 4, 5, 7\} \cup \{6, 9\} \\ &= \{1, 2, 4, 5, 6, 7, 9\}\end{aligned}$$

3. Consider the relation R on $\mathbb{Z}$ defined by aRb if and only if $3a =_{(7)} 3b$.

a) Are the following pairs in R? Circle the correct answer, no justification needed. [3 marks]

i) $(5, 4)$

ii) $(2, 9)$

iii) $(8, -1)$

b) Prove that R is an equivalence relation. [7 marks]

Answer(s)

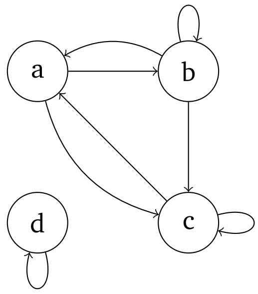
a) For each pair, we check whether $3a =_{(7)} 3b$ holds as if it does, then aRb, otherwise $a\not{R}b$.

- $(5, 4)$: We find $3 \cdot 5 - 3 \cdot 4 = 3$ is not divisible by 7 so $3a \neq_{(7)} 3b$ by definition.
- $(2, 9)$: We find $3 \cdot 2 - 3 \cdot 9 = -21$ is divisible by 7 so $3a =_{(7)} 3b$ by definition.
- $(8, -1)$: We find $3 \cdot 8 - 3 \cdot (-1) = 27$ is not divisible by 7 so $3a \neq_{(7)} 3b$ by definition.

b) To prove that R is an equivalence relation, we need to show that R is reflexive, symmetric and transitive.

- For all $a \in \mathbb{Z}$, we have $3a =_{(7)} 3a$ as $3a - 3a = 0$ is divisible by 7. Therefore, R is reflexive.
- Let $a, b \in \mathbb{Z}$ where aRb. Then, we have $3a =_{(7)} 3b$ so $7 \mid 3a - 3b$. We then find that $7 \mid 3b - 3a$ so $3b =_{(7)} 3a$ and therefore bRa. We find that R is symmetric.
- Let $a, b, c, d \in \mathbb{Z}$ where aRb and bRc. Then we have $3a =_{(7)} 3b$ and $3b =_{(7)} 3c$. This means $7 \mid 3a - 3b$ and $7 \mid 3b - 3c$. Hence, we have $7 \mid 3a - 3b + 3b - 3c = 3a - 3c$. By definition, we have $3a =_{(7)} 3c$ so aRc.

4. Consider the following directed graph representing a relation R on $A = \{a, b, c, d\}$:



a) Write the relation R as a set of ordered pairs. [4 marks]

b) Determine whether the following statements are true or false. [2 marks each]

i) R is reflexive.

ii) R is antisymmetric.

c) Calculate $R; R$. Express your answer as a set of ordered pairs. [2 marks]

Answer(s)

a) The relation R as a set of ordered pairs is:

$$R = \{(a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, c), (d, d)\}$$

b) i) **False**. R is not reflexive because (a, a) is not in R.

ii) **False**. R is not antisymmetric because both (a, b) and (b, a) are in R, but $a \neq b$.

c) The composition $R; R$ (i.e., R composed with itself) is calculated as follows:

For each pair (x, y) in R, find all pairs (y, z) in R and include the resulting pairs (x, z) in $R; R$. This gives:

$$R; R = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c), (d, d)\}$$

5. We define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $f(x, y) = (-y, x)$.

a) Find a function g such that $f \circ g = \mathrm{Id}_{\mathbb{Z}\times\mathbb{Z}} = g \circ f$. [4 marks]

b) Compute $h = f \circ f$. [2 marks]

c) Compute $h \circ h$. [2 marks]

d) Hence, give an integer n such that $g = f^n$. [2 marks]

Answer(s)

a) Let $a, b \in \mathbb{Z}$ such that $g(x, y) = (a, b)$ for integers x, y. Consider that

$$(f \circ g)(x, y) = f(g(x, y)) = f(a, b) = (-b, a).$$

We want $f \circ g = \mathrm{Id}_{\mathbb{Z}\times\mathbb{Z}}$, so we need $(-b, a) = (x, y)$. This means that $b = -x$ and $a = y$.

It seems that $g(x,y) = (y, -x)$ as $f \circ g = \mathrm{Id}_{\mathbb{Z}\times\mathbb{Z}}$. We now verify that $g \circ f = \mathrm{Id}_{\mathbb{Z}\times\mathbb{Z}}$ where

$$(g \circ f)(x,y) = g(f(x,y)) = g(-y,x) = (x, -(-y)) = (x,y).$$

We have $f \circ g = \mathrm{Id}_{\mathbb{Z}\times\mathbb{Z}} = g \circ f$ so g must be the inverse of f.

$$\begin{aligned} f(x,y) &= (-y,x) \\ g(x,y) &= (y,-x) \\ (f \circ g)(x,y) &= f(g(x,y)) = f(y,-x) = (x,y) \\ (g \circ f)(x,y) &= g(f(x,y)) = g(-y,x) = (x,y) \end{aligned}$$

b) For $h = f \circ f$, we compute:

$$h(x,y) = (f \circ f)(x,y) = f(f(x,y)) = f(-y,x) = (-x,-y).$$

c) For $h \circ h$, we compute:

$$(h \circ h)(x,y) = h(h(x,y)) = h(-x,-y) = (-(-x), -(-y)) = (x,y).$$

d) We compute successive powers of f to find that

$$\begin{aligned} f(x,y) &= (-y,x), \\ f^2(x,y) &= (f \circ f)(x,y) = (-x,-y),, \\ f^3(x,y) &= (f \circ f \circ f)(x,y) = f(-x,-y) = (y,-x). \end{aligned}$$

We find that $f^3(x,y) = (y,-x) = g(x,y)$ so $n = 3$.

6. a) Compute $(!1 \ \&\& \ 0) \ || \ (1 \ || \ (!0 \ \&\& \ 0))$. [1 mark]

b) Determine if the following are in Disjunctive Normal Form (DNF), Conjunctive Normal Form (CNF), or neither. [1 mark each]

i) $((b \ || \ (c \ \&\& \ !a)) \ || \ a) \ \&\& \ !c$

ii) $(a \ || \ (b \ || \ !c)) \ \&\& \ ((!a \ || \ c) \ \&\& \ (!a \ || \ b))$

iii) $(a \ \&\& \ !b) \ || \ (b \ \&\& \ (c \ || \ !a))$

c) Consider the following truth table for a boolean function $F(x,y,z)$:

x	y	z	$F(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

i) Give the canonical Disjunctive Normal Form (DNF) for F. [3 marks]

ii) Express F in DNF using the minimal number of minterms. [3 marks]

Answer(s)

a)

$$\begin{aligned}(!1 \mathbin{\&\&} 0) \mid\mid (1 \mid\mid (!0 \mathbin{\&\&} 0)) &= (0 \mathbin{\&\&} 0) \mid\mid (1 \mid\mid (1 \mathbin{\&\&} 0)) \\ &= 0 \mid\mid (1 \mid\mid (1 \mathbin{\&\&} 0)) \\ &= 0 \mid\mid (1 \mid\mid 0) \\ &= 0 \mid\mid 1 \\ &= 1\end{aligned}$$

b) i) $((b \mid\mid (c \mathbin{\&\&} !a)) \mid\mid a) \mathbin{\&\&} !c$: Neither

ii) $(a \mid\mid (b \mid\mid !c)) \mathbin{\&\&} ((!a \mid\mid c) \mathbin{\&\&} (!a \mid\mid b))$: CNF

iii) $(a \mathbin{\&\&} !b) \mid\mid (b \mathbin{\&\&} (c \mid\mid !a))$: Neither

c) i) The canonical DNF for F is

$$F(x, y, z) = (!x \mathbin{\&\&} y \mathbin{\&\&} !z) \mid\mid (x \mathbin{\&\&} !y \mathbin{\&\&} !z) \mid\mid (x \mathbin{\&\&} !y \mathbin{\&\&} z) \mid\mid (x \mathbin{\&\&} y \mathbin{\&\&} !z).$$

This expression is the OR of all minterms where $F(x, y, z) = 1$ in the truth table.

ii) Consider the Karnaugh map for this table:

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
x		+	+	+
$\bar{x}$		+		

The DNF with a minimal amount of minterms is $(y\bar{z}) \vee (x\bar{y})$

7. a) We have

$$\begin{aligned} p &= \text{“Today is Sunday”}, \\ q &= \text{“I am working”}, \\ r &= \text{“It is raining”}. \end{aligned}$$

Translate the following statements into logical notation. [1 mark each]

i) Today is Sunday and I am working.

ii) If it is raining, then I am not working.

b) Prove that the following logical argument is valid. [6 marks]

Today is Sunday and I am working
If it is raining then I am not working

Therefore, it is not raining

c) Prove or disprove the following logical equivalence. [2 marks]

$$(p \vee q) \to r \equiv (p \to r) \vee (q \to r)$$

Answer(s)

a) i) Today is Sunday and I am working: $p \land q$

ii) If it is raining, then I am not working: $r \to \neg q$

b) We first translate the argument into logical notation

$$\begin{array}{l} p \land q \\ r \to \neg q \\ \hline \neg r \end{array}$$

We will now draw the appropiate truth table

p	q	r	$\neg q$	$\neg r$	$p \land q$	$r \to \neg q$
F	F	F	T	T	F	T
F	F	T	T	F	F	T
F	T	F	F	T	F	T
F	T	T	F	F	F	F
T	F	F	T	T	F	T
T	F	T	T	F	F	T
T	T	F	F	T	T	T
T	T	T	F	F	T	F

From the truth table, when all the premises are true, the conclusion is true so the premises entail the conclusion. Hence, the argument is valid.

c) Consider the counterexample where p is true, but q and r are false. We get $(p \lor q) \to r$ is false, but, $(p \to r) \lor (q \to r)$ is true.

8. Prove, or find a counterexample to disprove:

a) For any sets $A, B,$ and $C,$ if $A \cap C \subseteq B \cap C,$ then $A \subseteq B.$ [5 marks]

b) For any sets A, B, we have $(A \setminus B) \cup (A \cap B) = A.$ [5 marks]

Answer(s)

a) Consider the counterexample where $A = \{1, 2\}$, $B = \{2\}$, and $C = \{2\}$. We have $A \cap C$ and $B \cap C = \{2\}$ so $A \cap C \subseteq B \cap C$. However, $A \not\subseteq B$ as $1 \in A$, but $1 \notin B$.

b) We can use set theory laws to prove this where

$$\begin{aligned}
(A \setminus B) \cup (A \cap B) &= (A \cap B^c) \cup (A \cap B) && \text{(Definition)} \\
&= A \cap (B^c \cup B) && \text{(Distributive law)} \\
&= A \cap (B \cup B^c) && \text{(Commutative law)} \\
&= A \cap U && \text{(Complement law)} \\
&= A && \text{(Identity law)}
\end{aligned}$$

Therefore, $(A \setminus B) \cup (A \cap B) = A$ for any sets A and B.

9. Let $\Sigma = \{a, b, c\}$ and define $f : \Sigma^* \times \Sigma^* \to \mathbb{Z}$ as

$$f(v, w) = \text{length}(v)\text{length}(w) - \text{length}(w).$$

a) Determine if f is injective. [3 marks]

b) Determine if f is surjective. [3 marks]

c) Show that $f(xy, z) = f(x, z) + f(y, z) + \text{length}(z)$. [4 marks]

Answer(s)

a) Consider $f(a, \lambda) = 0$ and $f(b, \lambda) = 0$, but, $(a, \lambda) \neq (b, \lambda)$ so f is not injective.

b) Note that $f(v, w) = (\text{length}(v) - 1) \cdot \text{length}(w)$.

- Let $n \in \mathbb{N}$. We find that $f(aa, a^n) = (\text{length}(aa) - 1) \cdot \text{length}(a^n) = (2 - 1) \cdot n = n$. Therefore, f can output all natural numbers.
- Let n be a negative integer. We find that $f(\lambda, a^{-n}) = (\text{length}(\lambda) - 1) \cdot \text{length}(a^{-n}) = (0 - 1) \cdot (-n) = n$. Therefore, f can output all negative integers.

Hence, the function f is surjective as it can output all integers.

c) Note that $\text{length}(xy) = \text{length}(x) + \text{length}(y)$. We have

$$\begin{aligned} f(xy, z) &= \text{length}(xy)\text{length}(z) - \text{length}(z), \\ &= (\text{length}(x) + \text{length}(y))\text{length}(z) - \text{length}(z), \\ &= \text{length}(x)\text{length}(z) + \text{length}(y)\text{length}(z) - \text{length}(z), \\ &= \text{length}(x)\text{length}(z) - \text{length}(z) + \text{length}(y)\text{length}(z) - \text{length}(z) + \text{length}(z), \\ &= f(x, z) + f(y, z) + \text{length}(z). \end{aligned}$$

10. Consider the relation $\lesssim$ on the set $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, where

$$x \lesssim y \text{ if and only if } x =_{(3)} y \text{ and } x \leq y.$$

a) Prove that $(A, \lesssim)$ is a partially ordered set [7 marks]

b) Draw the Hasse diagram for $(A, \lesssim)$ [3 marks]

Answer(s)

a) To prove that $(A, \lesssim)$ is a partially ordered set, we need to show that $\lesssim$ is reflexive, anti-symmetric, and transitive.

- For all $a \in A$, $a =_{(3)} a$ from the reflexivity of modular equivalence and $a \leq a$. By definition, we have $a \lesssim a$. Therefore, $\lesssim$ is reflexive.
- Let $a, b \in A$ where $a \lesssim b$ and $b \lesssim a$. By definition, we have $a =_{(3)} b$, $a =_{(3)} b$, $a \leq b$ and $b \leq a$. Since $\leq$ is anti-symmetric, we have $a = b$. Therefore, $\lesssim$ is anti-symmetric.
- Let $a, b, c \in A$ where $a \lesssim b$ and $b \lesssim c$. By definition, we have $a =_{(3)} b$, $b =_{(3)} c$, $a \leq b$ and $b \leq c$. We know that both $=_{(3)}$ and $\leq$ are transitive so we have $a =_{(3)} c$ and $a \leq c$. Therefore, $\lesssim$ is transitive.

b) The Hasse diagram for $(A, \lesssim)$ is:

$$\begin{array}{ccc} 9 & & \\ | & & \\ 6 & 7 & 8 \\ | & | & | \\ 3 & 4 & 5 \\ | & | & | \\ 0 & 1 & 2 \end{array}$$

Note: Elements in the same column are equivalent modulo 3 (i.e., $x =_{(3)} y$), and the vertical lines represent the $\leq$ relation.