

---

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING  
 COMP232 MATHEMATICS FOR COMPUTER SCIENCE  
 WINTER 2017

---

**Assignment 1. Solutions.**

---

1. For each of the following statements use a truth table to determine whether it is a tautology, a contradiction, or a contingency.

$$(a) \underbrace{((p \vee r) \wedge (q \vee r))}_{\mathbf{a}} \leftrightarrow \underbrace{((p \wedge q) \vee r)}_{\mathbf{c}}$$

**Solution:** Tautology.

$p$	$q$	$r$	$\mathbf{a}$ $\overbrace{p \vee r}$	$\mathbf{b}$ $\overbrace{q \vee r}$	$\mathbf{a} \wedge \mathbf{b}$	$p \wedge q$	$\mathbf{c}$ $\overbrace{(p \wedge q) \vee r}$	$(\mathbf{a} \wedge \mathbf{b}) \leftrightarrow \mathbf{c}$
$T$	$T$	$T$	$T$	$T$	$T$	$T$	$T$	$T$
$T$	$T$	$F$	$T$	$T$	$T$	$T$	$T$	$T$
$T$	$F$	$T$	$T$	$T$	$T$	$F$	$T$	$T$
$F$	$T$	$T$	$T$	$T$	$T$	$F$	$T$	$T$
$T$	$F$	$F$	$T$	$F$	$F$	$F$	$F$	$T$
$F$	$T$	$F$	$F$	$T$	$F$	$F$	$F$	$T$
$F$	$F$	$T$	$T$	$T$	$T$	$F$	$T$	$T$
$F$	$F$	$F$	$F$	$F$	$F$	$F$	$F$	$T$

$$(b) \underbrace{(p \wedge \underbrace{\neg(\neg p \vee q)}_{\mathbf{a}}))}_{\mathbf{b}} \vee \underbrace{(p \wedge q)}_{\mathbf{c}}$$

**Solution:** Contingency.

$p$	$q$	$\neg p$	$\neg p \vee q$	$\mathbf{a}$ $\overbrace{\neg(\neg p \vee q)}$	$\mathbf{b}$ $\overbrace{p \wedge \mathbf{a}}$	$\mathbf{c}$ $\overbrace{p \wedge q}$	$\mathbf{b} \vee \mathbf{c}$
$T$	$T$	$F$	$T$	$F$	$F$	$T$	$T$
$T$	$F$	$F$	$F$	$T$	$T$	$F$	$T$
$F$	$T$	$T$	$T$	$F$	$F$	$F$	$F$
$F$	$F$	$T$	$T$	$F$	$F$	$F$	$F$

$$(c) \underbrace{(p \wedge \underbrace{(\neg q \rightarrow \neg p)}_a)}_b \rightarrow q$$

**Solution:** Tautology.

$p$	$q$	$\neg p$	$\neg q$	$\underbrace{\neg q \rightarrow \neg p}_a$	$\underbrace{p \wedge a}_b$	$b \rightarrow q$
$T$	$T$	$F$	$F$	$T$	$T$	$T$
$T$	$F$	$F$	$T$	$F$	$F$	$T$
$F$	$T$	$T$	$F$	$T$	$F$	$T$
$F$	$F$	$T$	$T$	$T$	$F$	$T$

$$(d) \underbrace{(p \rightarrow r)}_a \vee \underbrace{(q \rightarrow r)}_b \rightarrow \underbrace{((p \vee q) \rightarrow r)}_c$$

**Solution:** Contingency.

$p$	$q$	$r$	$\underbrace{p \rightarrow r}_a$	$\underbrace{q \rightarrow r}_b$	$a \vee b$	$p \vee q$	$\underbrace{(p \vee q) \rightarrow r}_c$	$(a \vee b) \rightarrow c$
$T$	$T$	$T$	$T$	$T$	$T$	$T$	$T$	$T$
$T$	$T$	$F$	$F$	$F$	$F$	$T$	$F$	$T$
$T$	$F$	$T$	$T$	$T$	$T$	$T$	$T$	$T$
$F$	$T$	$T$	$T$	$T$	$T$	$T$	$T$	$T$
$T$	$F$	$F$	$F$	$T$	$T$	$T$	$F$	$F$
$F$	$T$	$F$	$T$	$F$	$T$	$T$	$F$	$F$
$F$	$F$	$T$	$T$	$T$	$T$	$F$	$T$	$T$
$F$	$F$	$F$	$T$	$T$	$T$	$F$	$T$	$T$

2. For each of the following logical equivalences state whether it is valid or invalid. If invalid then give a counterexample (*e.g.*, based on a truth table). If valid then give an algebraic proof using logical equivalences from Tables 6, 7, and 8 from Section 1.3 of textbook.

(a)  $p \rightarrow (q \rightarrow r) \equiv q \rightarrow (\neg p \vee r)$

**Solution:** Valid.

$$\begin{aligned}
 & p \rightarrow (q \rightarrow r) \\
 \equiv & \neg p \vee (q \rightarrow r) && \text{law for conditional} \\
 \equiv & \neg p \vee (\neg q \vee r) && \text{law for conditional} \\
 \equiv & (\neg p \vee \neg q) \vee r && \text{associativity} \\
 \equiv & (\neg q \vee \neg p) \vee r && \text{commutativity} \\
 \equiv & \neg q \vee (\neg p \vee r) && \text{associativity} \\
 \equiv & q \rightarrow (\neg p \vee r) && \text{law for conditional}
 \end{aligned}$$

(b)  $(p \rightarrow r) \wedge (q \rightarrow r) \equiv ((p \wedge q) \rightarrow r)$

**Solution:** Invalid.

If  $p = T$ ,  $q = F$ , and  $r = F$  then the LHS is False, while the RHS is True.

(c)  $(p \rightarrow q) \wedge (p \rightarrow r) \equiv (p \rightarrow (q \wedge r))$

**Solution:** Valid.

$$\begin{aligned}
 & (p \rightarrow q) \wedge (p \rightarrow r) \\
 \equiv & (\neg p \vee q) \wedge (\neg p \vee r) && \text{law for conditional} \\
 \equiv & \neg p \vee (q \wedge r) && \text{distributivity} \\
 \equiv & (p \rightarrow (q \wedge r)) && \text{law for conditional}
 \end{aligned}$$

(d)  $((p \vee q) \wedge (\neg p \vee r)) \equiv (q \vee r)$

**Solution:** Invalid.

If  $p = T$ ,  $q = T$ , and  $r = F$  then the LHS is False, while the RHS is True.

3. Write down the negations of each of the following statements *in their simplest form* (i.e., do not simply state “It is not the case that...”). Below,  $x$  denotes a real number,  $x \in \mathbb{R}$ .

(a) The plane is early or my watch is slow.

**Solution:** *The plane is on time and my watch is on time.*

This is of the form  $e \vee s$ . The negation is  $\neg(e \vee s) \equiv \neg e \wedge \neg s$ .

(b) Doing the assignments is a sufficient condition for John to pass the course.

**Solution:** *John does the assignments but does not pass the course.*

This is of the form  $a \rightarrow p$ . The negation is  $\neg(a \rightarrow p) \equiv a \wedge \neg p$ .

(c) If  $x$  is positive, then  $x$  is not negative and  $x$  is not 0.

**Solution:**  *$x$  is positive, and  $x$  is negative or  $x$  is 0.*

This is of the form  $p \rightarrow (\neg n \wedge \neg z)$ .

The negation is  $\neg(p \rightarrow (\neg n \wedge \neg z)) \equiv \neg p \vee \neg(\neg n \wedge \neg z) \equiv \neg p \vee n \vee z$ .

(d)  $(0 < x \leq 1) \vee (-1 < x < 0)$

**Solution:**  $(x = 0) \vee (x \leq 1) \vee (x > 1)$ .

The negation is that  $x$  does not lie in the half-open interval  $(0, 1]$  and  $x$  does not lie in the open interval  $(-1, 0)$

4. Write the following statements in predicate form, using logical operators  $\wedge$ ,  $\vee$ ,  $\neg$ , and quantifiers  $\forall$ ,  $\exists$ . Below  $\mathbb{Z}^+$  denotes all positive integers  $\{1, 2, 3, \dots\}$ .

We assume that the Universe of Discourse is all numbers (natural  $\mathbb{N}$ , integers  $\mathbb{Z}$ , rational  $\mathbb{Q}$ , irrational  $\mathbb{R}$ , complex  $\mathbb{C}$ , ...).

- (a) The square of a positive integer is always bigger than the integer.

**Solution:**  $\forall x (x \in \mathbb{Z}^+ \rightarrow x^2 > x)$

- (b) There is no integer solution to the equation  $x = x + 1$ .

**Solution:**  $\forall x (x \in \mathbb{Z} \rightarrow x \neq x + 1)$  or  $\neg [\exists x (x \in \mathbb{Z} \wedge x = x + 1)]$

- (c) The absolute value of an integer is not necessarily positive.

**Solution:**  $\exists x (x \in \mathbb{Z} \wedge |x| \not> 0)$

- (d) The absolute value of the sum of two integers does not exceed the sum of the absolute values of those integers.

**Solution:**  $\forall x \forall y ((x \in \mathbb{Z} \wedge y \in \mathbb{Z}) \rightarrow |x + y| \leq |x| + |y|)$

5. Let  $P$  and  $Q$  be predicates on the set  $S$ , where  $S$  has two elements, say,  $S = \{a, b\}$ . Then the statement  $\forall xP(x)$  can also be written in full detail as  $P(a) \wedge P(b)$ . Rewrite each of the statements below in a similar fashion, using  $P$ ,  $Q$ , and logical operators, but without using quantifiers.

$$(a) \quad \forall x, y(P(x) \vee Q(y)) \equiv \forall x(\forall y(P(x) \vee Q(y)))$$

**Solution:**

$$\begin{aligned} & \forall x(\forall y(P(x) \vee Q(y))) \\ \equiv & \quad \forall y(P(a) \vee Q(y)) \wedge \forall y(P(b) \vee Q(y)) \\ \equiv & \quad \left[ (P(a) \vee Q(a)) \wedge (P(a) \vee Q(b)) \right] \\ & \wedge \left[ (P(b) \vee Q(a)) \wedge (P(b) \vee Q(b)) \right] \\ & \wedge \left[ (P(c) \vee Q(a)) \wedge (P(c) \vee Q(b)) \right] \\ \equiv & \quad \left[ P(a) \vee (Q(a) \wedge Q(b)) \right] \\ & \wedge \left[ P(b) \vee (Q(a) \wedge Q(b)) \right] \\ & \wedge \left[ P(c) \vee (Q(a) \wedge Q(b)) \right] \end{aligned}$$

$$(b) \quad \exists xP(x) \vee \exists xQ(x)$$

**Solution:**

$$\begin{aligned} & \exists xP(x) \vee \exists xQ(x) \\ \equiv & \quad (P(a) \vee P(b)) \vee (\exists xQ(x)) \\ \equiv & \quad (P(a) \vee P(b)) \vee (Q(a) \vee Q(b)) \end{aligned}$$

$$(c) \quad \exists xP(x) \wedge \exists xQ(x)$$

**Solution:**

$$\begin{aligned} & \exists xP(x) \wedge \exists xQ(x) \\ \equiv & \quad (P(a) \vee P(b)) \wedge (\exists xQ(x)) \\ \equiv & \quad (P(a) \vee P(b)) \wedge (Q(a) \vee Q(b)) \end{aligned}$$

$$(d) \exists x, y(P(x) \wedge Q(y)) \equiv \exists x(\exists y(P(x) \wedge Q(y)))$$

**Solution:**

$$\begin{aligned} & \exists x(\exists y(P(x) \wedge Q(y))) \\ \equiv & \exists y(P(a) \wedge Q(y)) \vee \exists y(P(b) \wedge Q(y)) \\ \equiv & \left[ (P(a) \wedge Q(a)) \vee (P(a) \wedge Q(b)) \right] \\ & \vee \left[ (P(b) \wedge Q(a)) \vee (P(b) \wedge Q(b)) \right] \\ \equiv & \left[ P(a) \wedge (Q(a) \vee Q(b)) \right] \\ & \vee \left[ P(b) \wedge (Q(a) \vee Q(b)) \right] \end{aligned}$$

$$(e) \forall x \exists y(P(x) \wedge Q(y)) \equiv \forall x(\exists y(P(x) \wedge Q(y)))$$

**Solution:**

$$\begin{aligned} & \forall x(\exists y(P(x) \wedge Q(y))) \\ \equiv & \exists y(P(a) \wedge Q(y)) \wedge \exists y(P(b) \wedge Q(y)) \\ \equiv & \left[ (P(a) \wedge Q(a)) \vee (P(a) \wedge Q(b)) \right] \\ & \wedge \left[ (P(b) \wedge Q(a)) \vee (P(b) \wedge Q(b)) \right] \\ \equiv & \left[ P(a) \wedge (Q(a) \vee Q(b)) \right] \\ & \wedge \left[ P(b) \wedge (Q(a) \vee Q(b)) \right] \\ & \wedge \left[ P(c) \wedge (Q(a) \vee Q(b)) \right] \end{aligned}$$

6. Let the domain for  $x$  be the set of all students in this class and the domain for  $y$  be the set of all countries in the world. Let  $P(x, y)$  denote student  $x$  has visited country  $y$  and  $Q(x, y)$  denote student  $x$  has a friend in country  $y$ . Express each of the following using logical operations and quantifiers, and the propositional functions  $P(x, y)$  and  $Q(x, y)$ .

(a) Carlos has visited Bulgaria.

**Solution:**  $P(\text{Carlos}, \text{Bulgaria})$

(b) Every student in this class has visited the United States.

**Solution:**  $\forall x P(x, \text{UnitedStates})$

(c) Every student in this class has visited some country in the world.

**Solution:**  $\forall x \exists y P(x, y)$

(d) There is no country that every student in this class has visited.

**Solution:**  $\forall y \exists x \neg P(x, y)$

(e) There are two students in this class, who between them, have a friend in every country in the world.

**Solution:**  $\exists x \exists y (x \neq y \wedge \forall z [Q(x, z) \vee Q(y, z)])$

7. For each part in the previous question, form the negation of the statement so that all negation symbols occur immediately in front of predicates. For example:

$$\neg(\forall x(P(x) \wedge Q(x))) \equiv \exists x(\neg((P(x) \wedge Q(x)))) \equiv \exists x((\neg P(x)) \vee (\neg Q(x)))$$

- (a) **Solution:**  $\neg P(\text{Carlos}, \text{Bulgaria})$

*Carlos has not visited Bulgaria*

- (b) **Solution:**  $\neg(\forall x P(x, \text{UnitedStates})) \equiv \exists x(\neg P(x, \text{UnitedStates}))$

*There is a student in this class who has not visited the United States*

- (c) **Solution:**  $\neg(\forall x [\exists y P(x, y)]) \equiv \exists x \neg[\exists y P(x, y)] \equiv \exists x \forall y [\neg P(x, y)]$

*There is a student in this class who has not visited any country*

- (d) **Solution:**

$$\begin{aligned} \neg(\forall y [\exists x \neg P(x, y)]) &\equiv \\ \exists y \neg[\exists x \neg P(x, y)] &\equiv \\ \exists y \forall x \neg[\neg P(x, y)] &\equiv \\ \exists y \forall x [\neg\neg P(x, y)] &\equiv \\ \exists y \forall x P(x, y) & \end{aligned}$$

*There is a country that every student in this class has visited*

- (e) **Solution:**

$$\begin{aligned} \neg[\exists x (\exists y (x \neq y \wedge \forall z [Q(x, z) \vee Q(y, z)]))] &\equiv \\ \forall x \neg[\exists y (x \neq y \wedge \forall z [Q(x, z) \vee Q(y, z)])] &\equiv \\ \forall x [\forall y \neg(x \neq y \wedge \forall z [Q(x, z) \vee Q(y, z)])] &\equiv \\ \forall x [\forall y (x = y \vee \neg(\forall z [Q(x, z) \vee Q(y, z)]))] &\equiv \\ \forall x [\forall y (x = y \vee \exists z (\neg[Q(x, z) \vee Q(y, z)]))] &\equiv \\ \forall x [\forall y (x = y \vee \exists z (\neg Q(x, z) \wedge \neg Q(y, z)))] & \end{aligned}$$

*For every pair of distinct students in this class, there is a country where neither one of them has a friend*

8. Negate the following statements and transform the negation so that negation symbols immediately precede predicates. (See example in Question 7.)

$$(a) \exists x \exists y (P(x, y)) \vee \forall x \forall y (Q(x, y))$$

**Solution:**

$$\begin{aligned} & \neg(\exists x \exists y P(x, y) \vee \forall x \forall y Q(x, y)) \\ \equiv & \neg(\exists x \exists y P(x, y)) \wedge \neg(\forall x \forall y Q(x, y)) \\ \equiv & (\forall x \forall y \neg P(x, y)) \wedge (\exists x \exists y \neg Q(x, y)) \end{aligned}$$

$$(b) \forall x \forall y (Q(x, y) \leftrightarrow Q(y, x))$$

**Solution:**

$$\begin{aligned} & \neg(\forall x \forall y (Q(x, y) \leftrightarrow Q(y, x))) \\ \equiv & \exists x \exists y (\neg(Q(x, y) \leftrightarrow Q(y, x))) \\ \equiv & \exists x \exists y \neg((Q(x, y) \rightarrow Q(y, x)) \wedge (Q(y, x) \rightarrow Q(x, y))) \\ \equiv & \exists x \exists y (\neg(Q(x, y) \rightarrow Q(y, x)) \vee \neg(Q(y, x) \rightarrow Q(x, y))) \\ \equiv & \exists x \exists y (\neg(\neg Q(x, y) \vee Q(y, x)) \vee \neg(\neg Q(y, x) \vee Q(x, y))) \\ \equiv & \exists x \exists y ((Q(x, y) \wedge \neg Q(y, x)) \vee (Q(y, x) \wedge \neg Q(x, y))) \end{aligned}$$

$$(c) \forall y \exists x \exists z (T(x, y, z) \wedge Q(x, y))$$

**Solution:**

$$\begin{aligned} & \neg(\forall y \exists x \exists z (T(x, y, z) \wedge Q(x, y))) \\ \equiv & \exists y \forall x \forall z \neg(T(x, y, z) \wedge Q(x, y)) \\ \equiv & \exists y \forall x \forall z (\neg T(x, y, z) \vee \neg Q(x, y)) \end{aligned}$$

# COMP 232 Assignment 1 Solution

February 24, 2017

## Question 1

For each of the arguments below, formalize them in propositional logic. If the argument is valid identify which inference rule was used, and formulate the tautology underlying the rule. If the argument is invalid, state whether the inverse or converse error was made.

- a) All cheater sit in the back row.  
George sits in the back row.  
George is a cheater.

**Answer:**

$x$  consists of all the students.  $C(x)$ :  $x$  is a cheater.  $B(x)$ :  $x$  sits in the back row. Argument is in the form.

$$\frac{\forall x(C(x) \rightarrow B(x)) \quad B(\text{George})}{\therefore C(\text{George})}$$

Invalid, converse error.

- b) For all students  $x$ , if  $x$  studies discrete math, then  $x$  is good at logic.  
Dawn studies discrete math.  
Dawn is good at logic.

**Answer:**

$D(x)$ :  $x$  studies discrete math.  $L(x)$ :  $x$  is good at logic. Argument is in the form.

$$\frac{\forall x(D(x) \rightarrow L(x)) \quad D(\text{Dawn})}{\therefore L(\text{Dawn})}$$

Valid, universal instantiation and modus ponens.

- c) If the compilation of a computer program produces error messages, then the program is not correct or the compiler is faulty.  
The compilation of this program does not produce error messages.  
This program is correct and the compiler is not faulty.

**Answer:**

$e$ : produces error message.  $p$ : program is correct.  $c$ : the compiler is working. Argument is in the form.

$$\frac{e \rightarrow \neg p \vee \neg c}{\neg e} \\ \therefore p \wedge c$$

Invalid, inverse error.

- d) All students who do not do their homework and do not study the course material will not get a good course grade.

John gets a good course grade.

John did his homework or studied the course material.

**Answer:**

$x$  consists of all students.  $H(x)$ :  $x$  does the homework.  $S(x)$ ,  $x$  studies.  $G(x)$ ,  $x$  gets a good grade. Argument is in the form.

$$\frac{\forall x((\neg H(x) \wedge \neg S(x)) \rightarrow \neg G(x)) \\ G(\text{John})}{\therefore H(\text{John}) \vee S(\text{John})}$$

Valid, universal instantiation, contraposition, modus ponens, De Morgan's law, and double negation.

## Question 2

Use rules of inference to show that

a)

$$\frac{\forall x(R(x) \rightarrow (S(x) \vee Q(x))) \\ \exists x(\neg S(x))}{\therefore \exists x(R(x) \rightarrow Q(x))}$$

**Answer:**

**Step**

1.  $\forall x(R(x) \rightarrow (S(x) \vee Q(x)))$
2.  $\exists x(\neg S(x))$
3.  $R(a) \rightarrow (S(a) \vee Q(a))$
4.  $\neg R(a) \vee (S(a) \vee Q(a))$
5.  $(S(a) \vee Q(a)) \vee \neg R(a)$
6.  $S(a) \vee (Q(a) \vee \neg R(a))$
7.  $\neg S(a)$
8.  $Q(a) \vee \neg R(a)$
9.  $\neg R(a) \vee Q(a)$
10.  $R(a) \rightarrow Q(a)$
11.  $\exists x(R(x) \rightarrow Q(x))$

**Reason**

- Premise  
 Premise  
 Universal instantiation from 1  
 Logical equivalence from 3  
 Commutative law using 4  
 Associative law using 5  
 Existential instantiation from 2  
 Disjunctive syllogism using 6 and 7  
 Commutative law using 8  
 Logical equivalence from 9  
 Existential generalization from 10

b)

$$\frac{\forall x(P(x) \vee Q(x)) \\ \forall x((\neg P(x) \wedge Q(x)) \rightarrow R(x))}{\therefore \forall x(\neg R(x) \rightarrow P(x))}$$

**Answer:**

<b>Step</b>		<b>Reason</b>
1.	$\forall x(P(x) \vee Q(x))$	Premise
2.	$\forall x((\neg P(x) \wedge Q(x)) \rightarrow R(x))$	Premise
3.	$P(a) \vee Q(a)$	Universal instantiation from 1
4.	$(\neg P(a) \wedge Q(a)) \rightarrow R(a)$	Universal instantiation from 2
5.	$\neg(\neg P(a) \wedge Q(a)) \vee R(a)$	Logical equivalence from 4
6.	$(P(a) \vee \neg Q(a)) \vee R(a)$	De Morgan's law using 5
7.	$((P(a) \vee \neg Q(a)) \vee R(a)) \wedge (P(a) \vee Q(a))$	Conjunction using 6 and 3
8.	$((P(a) \vee \neg Q(a)) \vee R(a)) \wedge P(a)$ $\vee(((P(a) \vee \neg Q(a)) \vee R(a)) \wedge Q(a))$	Distributive law using 7
9.	$(P(a) \wedge ((P(a) \vee \neg Q(a)) \vee R(a)))$ $\vee(Q(a) \wedge ((\neg Q(a) \vee P(a)) \vee R(a)))$	Commutative law using 8
10.	$(P(a) \wedge (P(a) \vee (\neg Q(a) \vee R(a))))$ $\vee(Q(a) \wedge (\neg Q(a) \vee (P(a) \vee R(a))))$	Associative law using 9
11.	$P(a) \vee (Q(a) \wedge (\neg Q(a) \vee (P(a) \vee R(a))))$	Absorption law using 10
12.	$P(a) \vee ((Q(a) \wedge \neg Q(a)) \vee (Q(a) \wedge (P(a) \vee R(a))))$	Distributive law using 11
13.	$P(a) \vee (F \vee (Q(a) \wedge (P(a) \vee R(a))))$	Negation law using 12
14.	$P(a) \vee (Q(a) \wedge (P(a) \vee R(a)))$	Identity law using 13.
15.	$(P(a) \vee Q(a)) \wedge (P(a) \vee (P(a) \vee R(a)))$	Distributive law using 14
16.	$P(a) \vee (P(a) \vee (R(a)))$	Simplification from 15
17.	$(P(a) \vee P(a)) \vee R(a)$	Commutative law using 16
18.	$P(a) \vee R(a)$	Idempotent law using 17
19.	$R(a) \vee P(a)$	Commutative law using 18
20.	$\neg(\neg R(a) \vee P(a))$	Double negation law using 19
21.	$\neg R(a) \rightarrow P(a)$	Logical equivalence using 20.
22.	$\forall x(\neg R(x) \rightarrow P(x))$	Universal generalization using 21.

### Question 3

Prove that the product of two odd numbers is odd, using

- a) a direct proof;
- b) an indirect proof;
- c) a proof by contradiction.

**Answer:**

Let  $x$  and  $y$  be two odd numbers. We want to show  $xy$  is an odd number.

- a) Direct proof

By definition of odd number,  $x = 2a + 1$  and  $y = 2b + 1$  for some integers  $a$  and  $b$ . Then the product  $xy = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$ . We know that  $2ab + a + b$  is an integer. Thus,  $xy = 2(2ab + a + b) + 1$  is odd.

b) Indirect proof

Contraposition: If  $xy$  is the product of  $x$  and  $y$ , and  $xy$  is even; then  $x$  or  $y$  is even.

Assume  $x = 2a + c$  and  $y = 2b + d$ ,  $a$  and  $b$  are integers,  $c$  and  $d$  are either 0 or 1. Then  $xy = 4ab + 2ad + 2bc + cd = 2(2ab + ad + bc) + cd$ . Since  $xy$  is even, it has the form  $xy = 2e$  for some  $e$ . Thus,  $cd = 0$ . Therefore,  $x$  or  $y$  is even.

c) By contradiction

Assume  $x$  and  $y$  are odd, but  $xy$  is even.

By definition of odd  $x = 2a + 1$   $y = 2b + 1$  for some  $a$  and  $b$ . Then,  $xy = 2(2ab + a + b) + 1$  has the form of  $2c + 1$ , which is odd. But it contradicts to the assumption. Thus, if  $x$  and  $y$  are odd, then  $xy$  is odd.

## Question 4

For any integer  $n$ , prove that

a) 3 divides  $n^3 - n$

**Answer:**

$n^3 - n = n(n^2 - 1) = n(n + 1)(n - 1)$  Since  $n$  is an integer, then  $n - 1$ ,  $n$ , and  $n + 1$  are three consecutive integers. So, one of them is divisible by 3. Thus,  $n^3 - n$  is divisible by 3.

b) 3 divides one of the integers  $n$ ,  $n + 1$ , or  $2n + 1$

**Answer:**

If  $n$  or  $n + 1$  is divisible by 3, then the statement is true.

Otherwise,  $n - 1$  and  $n + 2$  are divisible by 3. Thus, the sum of  $n - 1$  and  $n + 2$  is  $2n + 1$  which is also divisible by 3.

c) 3 divides one of  $n$ ,  $n + 2$ , or  $n + 4$ .

**Answer:**

If  $n \equiv 0 \pmod{3}$ , then  $n$  is divisible by 3.

If  $n \equiv 1 \pmod{3}$ , then  $n - 1$  and  $n - 1 + 3 = n + 2$  is divisible by 3.

If  $n \equiv 2 \pmod{3}$ , then  $n - 2$  and  $n - 2 + 6 = n + 4$  is divisible by 3.

Therefore, the statement is true.

d) 3 divides one of  $n$ ,  $2n - 1$ , or  $2n + 1$ .

If  $n \equiv 0 \pmod{3}$ , then  $n$  is divisible by 3.

If  $n \equiv 1 \pmod{3}$ , then  $n - 1$  and  $n + 2$  are divisible by 3. Then  $n - 1 + n + 2 = 2n + 1$  is divisible by 3.

If  $n \equiv 2 \pmod{3}$ , then  $n - 2$  and  $n + 1$  are divisible by 3. Then  $n - 2 + n + 1 = 2n - 1$  is divisible by 3.

## Question 5

- a) Prove that  $\lfloor n/2 \rfloor \lceil n/2 \rceil = \lfloor n^2/4 \rfloor$  for all integers  $n$ . **Answer:**  
If  $n$  is even,  $n = 2a$  for some  $a$ . Then  $LHS = \lfloor 2a/2 \rfloor \lceil 2a/2 \rceil = a^2$ ,  
 $RHS = \lfloor 4a^2/4 \rfloor = a^2$ ,  
and  $LHS = RHS$ .  
If  $n$  is odd,  $n = 2a+1$  for some  $a$ . Then  $LHS = \lfloor (2a+1)/2 \rfloor \lceil (2a+1)/2 \rceil = a(a+1) = a^2 + a$ ,  
 $RHS = \lfloor (2a+1)^2/4 \rfloor = \lfloor (4a^2 + 4a + 1)/4 \rfloor = a^2 + a = LHS$ .

- b) Show that for any integer  $n$ ,  $5 \mid (n^5 - n)$ .

**Answer:**

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

If  $n = 5a$ , then  $n^5 - n = 5a(n-1)(n+1)(n^2 + 1)$ , which is divisible by 5.

If  $n = 5a + 1$ , then  $n - 1 = 5a$  and  $n^5 - n = n5a(n+1)(n^2 + 1)$ , which is divisible by 5.

If  $n = 5a + 2$ , then  $n - 2 = 5a$ ,  $n^2 + 1 = (n-2)(n+2) + 5 = 5(a(n+2) + 1)$ , and  $n^5 - n = n(n-1)(n+1)5(a(n+2) + 1)$ , which is divisible by 5.

If  $n = 5a + 3$ , then  $n - 3 = 5a$ ,  $n + 2 = 5(a+1)$ ,  $n^2 + 1 = (n-2)(n+2) + 5 = 5((n-2)(a+1) + 1)$ , and  $n^5 - n = n(n-1)(n+1)5((n-2)(a+1) + 1)$ , which is divisible by 5.

If  $n = 5a + 4$ , then  $n - 4 = 5a$ ,  $n + 1 = 5(a+1)$ , and  $n^5 - n = n(n-1)5(a+1)(n^2 + 1)$ , which is divisible by 5.

Thus, the statement is true for any integer.

- c) Show that if  $n$  is odd integer, then  $n^3 - n$  is a multiple of 24.

**Answer:**

Since  $n$  is odd,  $n = 2a + 1$  for some  $a$ .

$n^3 - n = n(n-1)(n+1) = 4a(a+1)(2a+1)$ . Thus, the original statement is equivalence to  $a(a+1)(2a+1)$  is divisible by 6.

If  $a = 6b$ , then it is done.

If  $a = 6b + 1$ ,  $a(a+1)(2a+1) = a2(3b+1)3(4b+1)$  is divisible by 6.

If  $a = 6b + 2$ ,  $a(a+1)(2a+1) = 2(3b+1)3(2b+1)(2a+1)$  is divisible by 6.

If  $a = 6b + 3$ ,  $a(a+1)(2a+1) = 3(2b+1)2(3b+2)(2a+1)$  is divisible by 6.

If  $a = 6b + 4$ ,  $a(a+1)(2a+1) = 2(3b+2)(a+1)3(4b+3)$  is divisible by 6.

If  $a = 6b + 5$ ,  $a(a+1)(2a+1) = a6(b+1)(2a+1)$  is divisible by 6.

Thus,  $a(a+1)(2a+1)$  is divisible by 6 for any  $a$ .

Thus, the original statement is true for any  $n$ .

## Question 6

For each of the statements below state whether it is True or False. If True then give a proof. If False then explain why, e.g., by giving a counterexample.

- a) For all positive  $x, y \in \mathbb{Q}$ , if  $x$  is irrational and  $y$  is irrational then  $x + y$  is irrational.

**Answer:** False, counterexample:  $x = \sqrt{2}$  and  $y = 2 - \sqrt{2}$ .

- b)  $\forall x, y \in \mathbb{Q}$ , if  $x$  is irrational and  $y$  is rational then  $x - y$  is irrational.

**Answer:** True.

Assume  $x$  is irrational and  $y$  is rational, but  $x - y$  is rational.  $y = a/b$  and  $x - y = c/d$ . Then  $x = y + (x - y) = a/b + c/d = (ad + bc)/bd$ , which is rational. But,  $x$  is irrational by assumption. This is a contradiction.

- c)  $\sqrt{3}$  is irrational.

**Answer:** True.

Assume  $\sqrt{3}$  is rational. Let  $\sqrt{3} = a/b$ . Then  $3 = a^2/b^2$ . Thus,  $3b^2 = a^2$ .  $a^2$  is divisible by 3.  $a$  is divisible by 3. So, let  $a = 3c$ . By substitution,  $3b^2 = 9c^2$ . Then,  $b^2 = 3c^2$ . This implies  $b$  is also divisible by 3. So,  $a, b$  have the common divisor 3, which is a contradiction.

- d)  $\log_5(2)$  is irrational.

**Answer:** True

Assume  $\log_5(2)$  is rational.  $\log_5(2) = a/b$ . Hence,

$$\begin{aligned} b \log_5(2) &= a \\ \log_5(2^b) &= a \\ 2^b &= 5^a \\ 5^a &= 2 * 2^{b-1} \end{aligned}$$

So,  $5^a$  is even and divisible by 2. But this is impossible, because  $5^a$  is only divisible by 5. Therefore, the assumption is false.

## Question 7

- a) Show that if  $x$  and  $y$  are positive rational numbers with  $x < y$  then there is a rational number  $r$  with  $x < r < y$ .

**Answer:**

Let  $a = \frac{y-x}{2}$ . Since  $x < y$ ,  $\frac{y-x}{2} > 0$ . Then, consider the number  $r = x + a$ .  $r - x = a > 0$  and  $y - r = a > 0$ . Thus,  $x < r < y$ .

b) Prove that if  $x$  is an integer then  $\lceil x \rceil = \lfloor x \rfloor$ .

**Answer:**

By definition of ceiling function  $\lceil x \rceil = x$  for integer  $x$ . And by definition of floor function  $\lfloor x \rfloor = x$  for integer  $x$ . Thus,  $\lceil x \rceil = \lfloor x \rfloor$  is true for any integer  $x$ .

c) Prove that if  $x$  is a real number but not an integer then  $\lceil x \rceil - \lfloor x \rfloor = 1$ .

**Answer:**

Since  $x$  is a real number but not an integer,  $0 < \lceil x \rceil - x < 1$  and  $0 < x - \lfloor x \rfloor < 1$ . So,  $\lceil x \rceil - \lfloor x \rfloor \in (0, 2)$ . We know that  $\lceil x \rceil$  and  $\lfloor x \rfloor$  are integers. So,  $\lceil x \rceil - \lfloor x \rfloor$  is also an integer. And there is only one integer in  $(0, 2)$ , which is 1. Thus,  $\lceil x \rceil - \lfloor x \rfloor = 1$ .

## Question 8

a) Prove that for any integer  $n$ ,  $n(n^2 - 1)(n + 2)$  is divisible by 12.

**Answer:**

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

Since,  $n - 1$ ,  $n$ ,  $n + 1$ , and  $n + 2$  are 4 consecutive integers, exactly one of them has to be divisible by 4, and at least one of them is divisible by 3. Thus, the product is divisible by 12.

b) Prove that  $n \in \mathbb{Z}^+$  is divisible by 3 if and only if the sum of its digits is divisible by 3.

**Answer:**

$$\text{Let } n = d_1 + 10d_2 + \cdots + 10^i d_i$$

$\Rightarrow$  By contradiction, assuming  $n$  is divisible by 3, but  $d_1 + d_2 + \cdots + d_i$  is not divisible by 3. Thus,

$$\begin{aligned}
d_1 + d_2 + \cdots + d_i &\equiv 1 \text{ or } 2 \pmod{3} \\
d_2 + \cdots + d_i &\equiv -d_1 + 1 \text{ or } -d_1 + 2 \pmod{3} \\
10(d_2 + \cdots + d_i) &\equiv -d_1 - 9d_1 + 10 \text{ or } -d_1 - 9d_1 + 20 \pmod{3} \\
10d_2 + \cdots + 10d_i &\equiv -d_1 + 1 \text{ or } -d_1 + 2 \pmod{3} \\
10d_3 + \cdots + 10d_i &\equiv -10d_2 - d_1 + 1 \text{ or } -10d_2 - d_1 + 2 \pmod{3} \\
10(10d_3 + \cdots + 10d_i) &\equiv -10 * 10d_2 - 10d_1 + 10 \text{ or } -10 * 10d_2 - 10d_1 + 20 \pmod{3} \\
100d_3 + \cdots + 100d_i &\equiv -10d_2 - 90d_2 - d_1 - 9d_1 + 1 + 9 \text{ or } -10d_2 - 90d_2 - d_1 - 9d_1 + 2 + 18 \pmod{3} \\
100d_3 + \cdots + 100d_i &\equiv -10d_2 - d_1 + 1 \text{ or } -10d_2 - d_1 + 2 \pmod{3} \\
&\vdots \\
0 &\equiv -(10^i + \cdots + 10d_2 + d_1) + 1 \text{ or } -(10^i + \cdots + 10d_2 + d_1) + 2 \pmod{3} \\
0 &\equiv -n + 1 \text{ or } -n + 2 \pmod{3} \\
n &\equiv 1 \text{ or } 2 \pmod{3}
\end{aligned}$$

This contradicts to  $n$  is divisible by 3.

$\Leftarrow$

$d_1 + d_2 + \cdots + d_i \equiv 0 \pmod{3}$ , then same as above.

c)  $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$

**Answer:**

If  $x$  is an integer,  $LHS = 3x$ ,  $RHS = x + x + x = 3x$ , and  $LHS = RHS$ .

If  $x$  is not an integer, let  $a = \lfloor x \rfloor$  and  $b = \{x\}$ . Then we have three cases for  $b$ .

If  $0 < b < \frac{1}{3}$ , then  $3b < 1$ ,  $b + \frac{2}{3} < 1$ ,  $LHS = \lfloor 3a + 3b \rfloor = 3a$ ,  $RHS = \lfloor a + b \rfloor + \lfloor a + b + \frac{1}{3} \rfloor + \lfloor a + b + \frac{2}{3} \rfloor = a + a + a = 3a$ , and  $LHS = RHS$ .

If  $\frac{1}{3} \leq b < \frac{2}{3}$ , then  $1 \leq 3b < 2$ ,  $b + \frac{1}{3} < 1$ ,  $1 \leq b + \frac{2}{3} < 2$ ,  $LHS = \lfloor 3a + 3b \rfloor = 3a + 1$ ,  $RHS = \lfloor a + b \rfloor + \lfloor a + b + \frac{1}{3} \rfloor + \lfloor a + b + \frac{2}{3} \rfloor = a + a + a + 1 = 3a + 1$ , and  $LHS = RHS$ .

If  $\frac{2}{3} \leq b < 1$ , then  $2 \leq 3b < 3$ ,  $1 \leq b + \frac{1}{3} < 2$ ,  $2 \leq b + \frac{2}{3} < 3$ ,  $LHS = \lfloor 3a + 3b \rfloor = 3a + 2$ ,  $RHS = \lfloor a + b \rfloor + \lfloor a + b + \frac{1}{3} \rfloor + \lfloor a + b + \frac{2}{3} \rfloor = a + a + 1 + a + 1 = 3a + 2$ , and  $LHS = RHS$ .

Thus,  $LHS = RHS$  for any  $x$ .

---

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING  
COMP232 MATHEMATICS FOR COMPUTER SCIENCE  
WINTER 2017

---

**Assignment 3. Solutions.**

---

1. For each of the following, determine whether it is valid or invalid. If valid then give a proof. If invalid then give a counter example.

(a)  $A \subseteq B \Rightarrow \overline{B} \subseteq \overline{A}$ .

**Solution:** Valid.

Assume  $A \subseteq B$ , and let  $x \in \overline{B}$ . Now  $x \in A$  or  $x \notin A$ . If  $x \in A$ , since  $A \subseteq B$  we get  $x \in B$ , a contradiction. Therefore it must be that  $x \notin A$ , that is,  $x \in \overline{A}$ .

(b)  $B \cap C \subseteq A \Rightarrow (C - A) \cap (B - A) = \emptyset$ .

**Solution:** Valid.

Proof by contradiction: Suppose  $B \cap C \subseteq A$ , and  $(C - A) \cap (B - A) \neq \emptyset$ . Then there exists an element  $x \in (C - A) \cap (B - A)$ . Thus this  $x$  satisfies  $x \in C$ ,  $x \in B$  and  $x \notin A$ . Thus  $x \in B \cap C$ , and since  $B \cap C \subseteq A$ , we get  $x \in A$ ; a contradiction.

2. Let  $f: \mathbb{R} \rightarrow \mathbb{Z}$ , where  $f(x) = \lceil 2x - 1 \rceil$ .

(a) Find  $f(A)$ , where  $A = \{x \in \mathbb{R} \mid 1 \leq x \leq 4\}$ .

**Solution:**  $f(A) = \{1, 2, 3, 4, 5, 6, 7\} = \{x \in \mathbb{Z} \mid 1 \leq x \leq 7\}$ .

(b) Find  $f^{-1}(B)$ , where  $B = \{-9, -8\}$ .

**Solution:**  $f^{-1}(B) = \{x \in \mathbb{R} \mid -9 \leq x < -7\}$ .

3. Give an example of a function

(a)  $f: \mathbb{Z} \rightarrow \mathbb{N}$  that is both 1-1 and onto.

**Solution:**

$$f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -(2n + 1) & \text{if } n < 0 \end{cases}$$

(b)  $f: \mathbb{N} \rightarrow \mathbb{Z}$  that is both 1-1 and onto.

**Solution:**

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ -(n+1)/2 & \text{if } n \text{ is odd} \end{cases}$$

4. Let  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  be defined as  $f(m, n) = (3m + 7n, 2m + 5n)$ . Is  $f$  a bijection, i.e., one-to-one and onto? If yes then give a formal proof, based on the definitions of one-to-one and onto, and derive a formula for  $f^{-1}$ . If no then explain why not.

**Solution:** The function  $f$  is a bijection.

Proof: To see that  $f$  is an injection, suppose  $f(m_1, n_1) = f(m_2, n_2)$ , that is,

$$3m_1 + 7n_1 = 3m_2 + 7n_2 \quad (1)$$

$$2m_1 + 5n_1 = 2m_2 + 5n_2 \quad (2)$$

Multiply Eq. (1) by 2 and Eq. (2) by 3, yielding

$$6m_1 + 14n_1 = 6m_2 + 14n_2 \quad (3)$$

$$6m_1 + 15n_1 = 6m_2 + 15n_2 \quad (4)$$

and then subtract Eq. (3) from Eq. (4), yielding  $n_1 = n_2$ . Substituting  $n_1 = n_2$  in Equation (1) yields  $m_1 = m_2$ .

To see that  $f$  is a surjection, let  $(k, \ell) \in \mathbb{Z} \times \mathbb{Z}$ . Then

$$3m + 7n = k \quad (5)$$

$$2m + 5n = \ell \quad (6)$$

Multiplying Eq. (5) by 2 and Eq. (6) by 3 yields

$$6m + 14n = 2k \quad (7)$$

$$6m + 15n = 3\ell \quad (8)$$

Subtracting Eq. (7) from Eq. (8) yields

$$n = 3\ell - 2k \quad (9)$$

Multiplying Eq. (5) by 3 and Eq. (6) by 4 yields

$$9m + 21n = 3k \quad (10)$$

$$8m + 20n = 4\ell \quad (11)$$

Subtracting (11) from (10) yields

$$m + n = 3k - 3\ell \quad (12)$$

Substituting (9) in (12) yields

$$m = 5k - 6\ell \quad (13)$$

We can thus see that for each pair  $(k, \ell) \in \mathbb{Z} \times \mathbb{Z}$  there is a pair  $(5k - 6\ell, 3\ell - 2k) \in \mathbb{Z} \times \mathbb{Z}$  such that,  $f((5k - 6\ell, 3\ell - 2k)) = (k, \ell)$ . So,  $f$  is a surjective function.

After proving  $f$  is surjective, deriving a formula for  $f^{-1}$  is not difficult anymore. Here we have:  $f^{-1}(k, \ell) = (5k - 6\ell, 3\ell - 2k)$ .

5. (a) Suppose that Hilbert's Grand Hotel is fully occupied, but the hotel closes all even numbered rooms for maintenance. Show that all guests can remain in the hotel.

**Solution:** Move guest in room  $n$  to room  $2n - 1$ .

- (b) Show that a countably infinite number of guests arriving at Hilbert's fully occupied Grand Hotel can be given rooms without evicting any current guest.

**Solution:** First move old guest from room  $n$  to room  $2n - 1$ . Then all even-numbered rooms are free. Now you can put new guest  $n$  in room  $2n$ .

6. If  $f$  and  $f \circ g$  are one-to-one, does it follow that  $g$  is one-to-one? Justify your answer.

**Solution:** Yes.

Proof by contradiction: Suppose that  $f$  and  $f \circ g$  are one-to-one, and that  $g$  is not one-to-one. Then there are  $a, b \in A$ , such that  $a \neq b$  and  $g(a) = g(b)$ . Since  $f$  is one-to-one, we have  $f(g(a)) = f(g(b))$ . But  $f \circ g(a) = f(g(a)) = f(g(b)) = f \circ g(b)$ , contradicting the assumption that  $f \circ g$  is one-to-one.

7. Let  $A = \{1, 2, 3, 4, 5\}$ .

- (a) How many total functions  $f : A \rightarrow A$  are there?

**Solution:**

Each of the five elements in  $A$  can be mapped (independently of how the other elements in  $A$  are mapped) to any of the five elements in  $A$ . Consequently, there are  $5^5 = 3125$  possible functions  $f : A \rightarrow A$ .

- (b) How many of the functions in (a) are one-to-one?

**Solution:**

Suppose a function  $f$  maps 1 to any of the five elements in  $A$ . Then there are four choices left for mapping 2, three choices for 3, two choices for 4, and one choice for 5. Consequently, each of the  $5! = 120$  permutations of 1, 2, 3, 4, 5 represents a one-to-one function on  $A$ .

8. Suppose  $f : \mathbb{R} \rightarrow \mathbb{R}$  and  $g : \mathbb{R} \rightarrow \mathbb{R}$  where  $g(x) = 2x + 1$  and  $g \circ f(x) = 2x + 11$ . Find the rule for  $f$ .

**Solution:**

We know that  $g(x) = 2x + 1$ , and  $g \circ f(x) = 2x + 11$ . Let  $f(x) = ax + b$ , then we have

$$g \circ f(x) = g(f(x)) = 2(ax + b) + 1,$$

so we have

$$2(ax + b) + 1 = 2x + 11$$

consequently,

$$2(ax + b) + 1 = 2ax + 2b + 1 = 2x + 11$$

which implies that

$$2a = 2 \Rightarrow a = 1$$

$$2b + 1 = 11 \Rightarrow b = 5$$

finally we have

$$f(x) = x + 5.$$

9. Prove or disprove the statements below.

- (a) For all positive real numbers  $x$  and  $y$ ,  $\lfloor x \cdot y \rfloor \leq \lfloor x \rfloor \cdot \lfloor y \rfloor$ .

**Solution:** The claim is false.

Counter-example:  $x = y = 1.5$ . Then  $\lfloor x \cdot y \rfloor = \lfloor 1.5 \cdot 1.5 \rfloor = \lfloor 2.25 \rfloor = 2$ , and  $\lfloor x \rfloor \cdot \lfloor y \rfloor = \lfloor 1.5 \rfloor \cdot \lfloor 1.5 \rfloor = 1 \cdot 1 = 1$ .

- (b) For all positive real numbers  $x$  and  $y$ ,  $\lceil x \cdot y \rceil \leq \lceil x \rceil \cdot \lceil y \rceil$ .

**Solution:** The claim is true.

Proof: We have  $x \leq \lceil x \rceil$  and  $y \leq \lceil y \rceil$ , and thus  $x \cdot y \leq \lceil x \rceil \cdot \lceil y \rceil$ . Consequently  $\lceil x \cdot y \rceil \leq \lceil \lceil x \rceil \cdot \lceil y \rceil \rceil = \lceil x \rceil \cdot \lceil y \rceil$ .

10. (a) Show that if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , where  $a, b, c, d$ , and  $m$  are integers with  $m \geq 2$ , then  $a - c \equiv b - d \pmod{m}$ .

**Solution:**  $a \equiv b \pmod{m}$  means that  $\exists k \in \mathbb{Z}$ , such that  $a = b + km$ . Likewise,  $c = d + k'm$ , for some  $k' \in \mathbb{Z}$ . Thus  $a - c = b - d + km - k'm = b - d + (k - k')m$ , which means that  $a - c \equiv b - d \pmod{m}$ .

- (b) Show that if  $a, b, k$  and  $m$  are integers such that  $k \geq 1$ ,  $m \geq 2$ , and  $a \equiv b \pmod{m}$ , then  $a^k \equiv b^k \pmod{m}$

**Solution:** Since  $a \equiv b \pmod{m}$ , we have

$$a = b + p_1 \cdot m,$$

for some  $p_1 \in \mathbb{Z}$ . We shall show by an induction on  $k$  that for each  $k$  there is a  $p_k \in \mathbb{Z}$ , such that  $a^k = b^k + p_k \cdot m$ . The claim then follows.

The base case  $k = 1$  is the assumption. For the inductive hypothesis, suppose the claim holds for some  $k$ , that is

$$a^k = b^k + p_k \cdot m$$

for some  $p_k \in \mathbb{Z}$ . We need to show that it holds for  $k + 1$ . We have

$$\begin{aligned} a \cdot a^k &= \\ (b + p_1 \cdot m)(b^k + p_k \cdot m) &= \\ b^{k+1} + b \cdot p_k \cdot m + p_1 \cdot m \cdot b^k + p_1 \cdot m \cdot p_k \cdot m &= \\ b^{k+1} + (b \cdot p_k + p_1 \cdot b^k + p_1 \cdot m \cdot p_k) \cdot m & \end{aligned}$$

In other words,

$$a^{k+1} = b^{k+1} + \underbrace{(b \cdot p_k + p_1 \cdot b^k + p_1 \cdot m \cdot p_k)}_{p_{k+1}} \cdot m.$$

# COMP 232 Assignment 4 Solution

## Question 1

Base case:

$$n = 18, 18 = 7 + 7 + 4;$$

$$n = 19, 19 = 7 + 4 + 4 + 4;$$

$$n = 20, 20 = 4 + 4 + 4 + 4 + 4;$$

$$n = 21, 21 = 7 + 7 + 7.$$

Inductive hypothesis: assume when  $18 \leq n \leq k$ ,  $n$  is a sum of 4's and 7's.

Inductive step: we need to show when  $n = k + 1$ , the statement is true.

From IH, we know  $n = k - 3$  is a sum of 4's and 7's. Thus,  $n = k - 3 + 4 = k + 1$  is also a sum of 4's and 7's.

Thus, the statement is true for all  $n \geq 18$ .

## Question 2

1.  $S = \{(a, b) : a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } a + b \text{ is odd}\}$  Solution:

- Base case 1:  $(1, 2) \in S$ .
- Base case 2:  $(2, 1) \in S$ .
- Recursive case 1: if  $(i, j) \in S$  then  $(i + 1, j + 1) \in S$ .
- Recursive case 2: if  $(i, j) \in S$  then  $(i, j + 2) \in S$ .
- Recursive case 3: if  $(i, j) \in S$  then  $(i + 2, j) \in S$ .

2.  $S = \{(a, b) : a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } a|b\}$  Solution:

- Base case:  $(n, n) \in S$  for all  $n \in \mathbb{Z}^+$ .
- Recursive case: if  $(i, j) \in S$  then  $(i, j \cdot k) \in S$ , for all  $k \in \mathbb{Z}^+$ .

3.  $S = \{(a, b) : a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } 3|(a + b)\}$  Solution:

- Base case 1:  $(1, 2) \in S$ .
- Base case 2:  $(2, 1) \in S$ .
- Recursive case 1: if  $(i, j) \in S$  then  $(i + 3, j) \in S$ .
- Recursive case 2: if  $(i, j) \in S$  then  $(i, j + 3) \in S$ .

- Recursive case 3: if  $(i, j) \in S$  then  $(i + 1, j + 2) \in S$ .
- Recursive case 4: if  $(i, j) \in S$  then  $(i + 2, j + 1) \in S$ .

### Question 3

Base case:  $n = 1$ ,  $LHS = 1 \cdot 1! = 1$ ,  $RHS = (1 + 1)! - 1 = 2 - 1 = 1$ . Thus,  $LHS = RHS$ .

Inductive hypothesis: Assume when  $n = k$ , the statement  $1 \cdot 1! + 2 \cdot 2! + \dots + k \cdot k! = (k + 1)! - 1$  is true.

Inductive step: We need to show  $1 \cdot 1! + 2 \cdot 2! + \dots + k \cdot k! + (k + 1) \cdot (k + 1)! = (k + 2)! - 1$

$$\begin{aligned}
 LHS &= (k + 1)! - 1 + (k + 1) \cdot (k + 1)! \\
 &= (k + 1)!(1 + k + 1) - 1 \\
 &= (k + 2)! - 1 \\
 &= RHS
 \end{aligned}$$

Thus, the statement is true for all  $n \geq 1$ .

### Question 4

Base case: when  $n = 1$ ,  $4^{1+1} + 5^{2-1} = 21 \equiv 0 \pmod{21}$ .

Inductive hypothesis: assume when  $n = k$ ,  $4^{k+1} + 5^{2k-1} \equiv 0 \pmod{21}$ .

Inductive step:

By inductive hypothesis:

$$\begin{aligned}
 4^{k+1} + 5^{2k-1} &\equiv 0 \pmod{21} \\
 4^{k+1} + 5^{2k-1} &= 21a \\
 5^{2k-1} &= 21a - 4^{k+1}
 \end{aligned}$$

The equivalence we want to show:

$$\begin{aligned}
 &4^{k+1+1} + 5^{2(k+1)-1} \\
 &= 4 \cdot 4^{k+1} + 25 \cdot 5^{2k-1} \\
 &= 4 \cdot 4^{k+1} + 25(21a - 4^{k+1}) \text{ by substitution} \\
 &= 21 \cdot 4^{k+1} + 25 \cdot 21a \\
 &= 21(4^{k+1} + 25a) \\
 &\equiv 0 \pmod{21}
 \end{aligned}$$

### Question 5

Base case:

when  $n = 1$ ,  $f_{4n} = f_4 = 3 \equiv 0 \pmod{3}$ .

Inductive hypothesis: assume  $n = k$ ,  $f_{4n} \equiv 0 \pmod{3}$ .

Inductive step: when  $n = k + 1$

$$\begin{aligned}f_{4k+4} &= f_{4k+3} + f_{4k+2} \\ &= f_{4k+2} + 2f_{4k+1} + f_{4k} \\ &= f_{4k+1} + 2f_{4k-1} + 4f_{4k} \\ &= 5f_{4k} + 3f_{4k-1}\end{aligned}$$

From inductive hypothesis, we know  $5f_{4k} \equiv 0 \pmod{3}$ . And  $3f_{4k-1} \equiv 0 \pmod{3}$ . Thus,  $f_{4k+4} \equiv 0 \pmod{3}$ .

## Question 6

Base case: when  $n = 2$ ,  $LHS = f_{2-1}f_{2+1} - f_2^2 = 1 \times 2 - 1 = 1 = 1^2 = RHS$ .

Inductive hypothesis: assume when  $n = k$ ,  $f_{k-1}f_{k+1} - f_k^2 = (-1)^k$ .

Inductive step: when  $n = k + 1$ ,

$$\begin{aligned}f_k f_{k+2} - f_{k+1}^2 &= f_k(f_k + f_{k+1}) - f_{k+1}^2 \\ &= f_k^2 + f_k f_{k+1} - f_{k+1}^2 \\ &= f_k^2 - f_{k+1}(f_{k+1} - f_k) \\ &= f_k^2 - f_{k+1}(f_k + f_{k-1} - f_k) \\ &= f_k^2 - f_{k+1}f_{k-1} \\ &= -(-1)^k \\ &= (-1)^{k+1}\end{aligned}$$

Thus, the statement is true for all  $n \geq 2$ .

## Question 7

	Reflexive	Symmetric	Antisymmetric	Transitive
a	No	No	Yes	No
b	No	No	Yes	No
c	Yes	Yes	No	Yes
d	No	Yes	No	No
e	Yes	Yes	No	No
f	No	Yes	No	No
g	Yes	No	Yes	Yes
h	No	Yes	No	No

### Question 8

a. 
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

b. 
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

### Question 9

a)  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

b)  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

c)  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix},$   
 $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

d)  $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},$   
 $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

### Question 10

$$\begin{aligned} [1] &= \{1, 7, 11, 13\} \\ [2] &= \{2, 4, 8, 14\} \\ [3] &= \{3, 9\} \\ [5] &= \{5\} \\ [6] &= \{6, 12\} \\ [10] &= \{10\} \\ [15] &= \{15\} \end{aligned}$$

### **Question 11**

- a) Yes
- b) Yes
- c) Yes
- d) No

### **Question 12**

- a) Yes
- b) No
- c) Yes
- d) No