CONCORDIA UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

COMP232 MATHEMATICS FOR COMPUTER SCIENCE

ASSIGNMENT 2 SOLUTIONS FALL 2011

1. Prove that if x^5 is irrational then x is irrational, by proving the contrapositive.

   PROOF: The contrapositive is "*If x is rational then x^5 is rational*". To prove this assume that $x = \frac{p}{q}$, where p and q are integers. Then $x^5 = \frac{p^5}{q^5}$, which is a rational number.

2. Give a proof by cases to show that there are no integer solutions to the equation

$$2x^2 \ + \ 5y^2 \ = \ 14 \ .$$

   PROOF: We have $2x^2 \leq 14$, *i.e.*, $x^2 \leq 7$, *i.e.*, $\mid x \mid \leq 2$ (since x is an integer), and $5y^2 \leq 14$, *i.e.*, $y^2 \leq 2.8$, *i.e.*, $\mid y \mid \leq 1$. There remain 6 cases to be considered, namely, $x = 0, 1, 2$, combined with $y = 0, 1$. (Negative x and y need not be considered separately.) It is easily checked that none of these 6 combinations of x and y satisfy the equation.

3. Give a proof by contradiction to show that the cube root of 3 is an irrational number.

   PROOF: Suppose $3^{1/3}$ is rational, *i.e.*, $3^{1/3} = p/q$, where p and q are relatively prime (*i.e.*, p and q only have 1 as common factor.) Then $3 = p^3/q^3$, or, $p^3 = 3q^3$. Thus $3|p^3$. Hence $3|p$, say, $p = 3k$ for some integer k. Then $3q^3 = (3k)^3 = 3^3k^3$, or, $q^3 = 3^2k^3$. Thus $3|q^3$, hence $3|q$. So p and q have 3 as common factor. Contradiction.

   NOTE: We used the fact that if $3|n^3$ then $3|n$, whose contrapositive is easily proved by cases: If $3 \not| n$ then $n = 3k + 1$ or $n = 3k + 2$, hence $n^3 = (3k + 1)^3 = 3(9k^3 + 9k^2 + 3k) + 1$ or $n^3 = (3k + 2)^3 = 3(9k^3 + 18k^2 + 12k + 2) + 2$, both of which are not divisible by 3.

4. Give a proof by contradiction to show that if the integers 1, 2, $\cdots$, 99, 100 , are placed randomly around a circle (without repetition), then there must exist three adjacent numbers along the circle whose sum is greater than 152.

   PROOF: Suppose the sum of any three adjacent numbers is less than or equal to 152. The number 1 must be somewhere along the circle. The remaining 99 positions can be grouped in 33 *nonintersecting groups* of 3 adjacent positions. Then the total sum will be less than or equal to $33 \cdot 152 + 1 = 5017$. However, we know that $1 + 2 + ... + 100 = 100 * 101/2 = 5050$. Contradiction.

5. Prove the following by contradiction:

   (a) There is no least positive rational number.

   PROOF: Suppose $r_1 = \frac{p}{q}$ is the least rational number. Let $r_2 = \frac{2p-1}{2q}$. Then r_2 is rational, and $r_2 < r_1$. Contradiction.

(b) For all real numbers x and y, if x is irrational and y is rational then $x - y$ is irrational.

PROOF: Suppose x is irrational, and y is rational, say, $y = \frac{p_1}{q_1}$, but $x - y$ is rational, say, $x - y = \frac{p_2}{q_2}$, where p_1, q_1, p_2 and q_2 are positive integers. Then $x = y + \frac{p_2}{q_2} = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}$. Hence x is rational. Contradiction.

(c) $\log_5(2)$ is irrational.

PROOF: Suppose $\log_5(2)$ is rational, say, $\log_5(2) = p/q$, where p and q are positive integers. Then, by definition of logarithm, $5^{p/q} = 2$, from which $5^p = 2^q$. But 5^p is odd, while 2^q is even. Contradiction.

6. Let n be an integer. Prove that the following statements are equivalent:

$$n^3 \text{ is odd} , \qquad n^2 \text{ is odd} , \qquad 1 - n \text{ is even} , \qquad n^2 + 1 \text{ is even} .$$

PROOF: Re-order the above as

(a) $1 - n$ is even , (b) n^2 is odd , (c) $n^2 + 1$ is even , (d) n^3 is odd .

To establish equivalence it suffices to prove that

$$(a) \Rightarrow (b) , \qquad (b) \Rightarrow (c) , \qquad (c) \Rightarrow (d) , \quad \text{and} \quad (d) \Rightarrow (a) .$$

$(a) \Rightarrow (b)$: If $1 - n$ is even then $1 - n = 2k_1$ for some integer k_1. Hence $n = -2k_1 + 1$ so that n is odd. Then $n^2 = (-2k_1 + 1)^2 = 2(2k_1^2 - 2k_1) + 1$, so n^2 is odd.

$(b) \Rightarrow (c)$: Since n^2 is odd we have $n^2 = 2k_2 + 1$. Thus $n^2 + 1 = 2k_2 + 2 = 2(k_2 + 1)$, so that $n^2 + 1$ is even.

$(c) \Rightarrow (d)$: If $n^2 + 1$ is even then (easily) n^2 is odd, $n^2 = 2k_3 + 1$. Also, if n is even then (easily) n^2 is even, or (contrapositive) if n^2 is odd then n is odd, *i.e.*, $n = 2k_4 + 1$. Now $n^3 = n^2\ n = (2k_3 + 1)(2k_4 + 1) = 2(2k_3k_4 + k_3 + k_4) + 1$, so that n^3 is odd.

$(d) \Rightarrow (a)$: We prove the contrapositive: If $1 - n$ is odd then n^3 is even. Now if $1 - n$ is odd then (easily) n is even, say, $n = 2k_5$. Hence $n^3 = 2(4k_5^3)$ is even.

7. Taking $a(x)$, $b(x)$ and $c(x)$ to denote the statements "$x \in A$", "$x \in B$" and "$x \in C$" respectively, write each of the following as a proposition in predicate logic, then prove the proposition is valid.

(a) $A \cup B \;=\; A \cup (B - A)$

(b) $(A \cup B) \subseteq C \;\equiv\; (A \subseteq C) \;\wedge\; (B \subseteq C)$

SOLUTION:

(a) We must prove

$$\big(a(x) \vee b(x)\big) \;\equiv\; \big(a(x) \vee (b(x) \wedge \neg a(x))\big) .$$

It suffices to prove that, for arbitrary logical variables a and b, we have

$$a \vee b \;\equiv\; a \vee (b \wedge \neg a).$$

Starting with the RHS we have $a \vee (b \wedge \neg a) \;\equiv\; (a \vee b) \wedge (a \vee \neg a) \;\equiv\; (a \vee b) \wedge T \;\equiv\; a \vee b$.

(b) Similarly, here we must prove that for arbitrary logical variables a, b and c we have

$$\big((a \vee b) \rightarrow c\big) \;\equiv\; (a \rightarrow c) \wedge (b \rightarrow c).$$

Starting with the LHS we have $\big((a \vee b) \rightarrow c\big) \;\equiv\; \neg(a \vee b) \vee c \;\equiv\; (\neg a \wedge \neg b) \vee c$

$\equiv\; c \vee (\neg a \wedge \neg b) \;\equiv\; (c \vee \neg a) \wedge (c \vee \neg b) \;\equiv\; (a \rightarrow c) \wedge (b \rightarrow c).$

8. 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) $B \cap C \subseteq A \;\Rightarrow\; (C - A) \cap (B - A)$ is empty

(b) $(A \cup B) - (A \cap B) = A \;\Rightarrow\; B$ is empty

SOLUTION:

(a) This statement is valid. We prove the contrapositive:

If $(C - A) \cap (B - A)$ is not empty then $B \cap C$ is not a subset of A.

PROOF: Since $(C-A)\cap(B-A)$ is not empty there is an x such that $x \in (C-A)\cap(B-A)$, *i.e.*, $x \in C$ and $x \in B$ and $x \notin A$. Thus $x \in B \cap C$ and $x \notin A$. Thus $B \cap C$ is not a subset of A.

(b) This statement is also valid. We prove the contrapositive:

If B is not empty then $(A \cup B) - (A \cap B) \neq A$.

To prove the contrapositive we use a proof by contradiction: Suppose B is not empty, but $(A \cup B) - (A \cap B) = A$. Then there exists an element $b \in B$. There are two cases to consider:

Case 1: $b \in A$: Then $b \in A \cup B$ and $b \in A \cap B$. Hence $b \notin (A \cup B) - (A \cap B)$. Thus, using our assumption that $(A \cup B) - (A \cap B) = A$ it follows that $b \notin A$, which is a contradiction.

Case 2: $b \notin A$: In this case $b \in A \cup B$, but $b \notin A \cap B$. Hence $b \in (A \cup B) - (A \cap B)$. Using our assumption that $(A \cup B) - (A \cap B) = A$, it follows that $b \in A$, which is a contradiction.

9. Let

$$f(x) \;=\; ax \;+\; b \qquad \text{and} \qquad g(x) \;=\; cx \;+\; d\,,$$

where a, b, c, and d are real constants. Determine for which constants a, b, c, and d it is true that

$$f \circ g \;=\; g \circ f\ .$$

SOLUTION:

$$f(g(x)) \;=\; f(cx + d) \;=\; a(cx + d) + b \;=\; acx + ad + b\ ,$$

and

$$g(f(x)) \;=\; g(ax + b) \;=\; c(ax + b) + d \;=\; acx + bc + d\ .$$

We see that $f(g(x)) = g(f(x))$ for all x if and only if

$$ad + b \;=\; bc + d\ .$$

10. Let x be a real number. Prove that

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

PROOF: Let $x = n + r$, where $0 \le r < 1$, and consider the following three cases:

$0 \le r < 1/3$: Then $\lfloor 3x \rfloor = 3n$, $\lfloor x \rfloor = n$, $\lfloor x + \frac{1}{3} \rfloor = n$, $\lfloor x + \frac{2}{3} \rfloor = n$.

$1/3 \le r < 2/3$: Then $\lfloor 3x \rfloor = 3n + 1$, $\lfloor x \rfloor = n$, $\lfloor x + \frac{1}{3} \rfloor = n$, $\lfloor x + \frac{2}{3} \rfloor = n + 1$.

$2/3 \le r < 1$: Then $\lfloor 3x \rfloor = 3n + 2$, $\lfloor x \rfloor = n$, $\lfloor x + \frac{1}{3} \rfloor = n + 1$, $\lfloor x + \frac{2}{3} \rfloor = n + 1$.

In each of these three cases the identity holds.

11. Let f be a one-to-one function from the set A to the set B . Let S and T be subsets of A . Prove that

$$f(S \cap T) \;=\; f(S) \cap f(T)\ .$$

PROOF: If $b \in f(S \cap T)$ then there is an element $a \in S \cap T$ such that $f(a) = b$. Since $a \in S$ we have $b \in f(S)$. Since $a \in T$ we have $b \in f(T)$. Thus $b \in f(S) \cap f(T)$. Thus we have shown that $f(S \cap T) \subseteq f(S) \cap f(T)$.

To prove the converse we need the assumption that f is one-to-one. Arguing by contradiction, suppose that the converse does not hold, *i.e.*, f is one-to-one, but $f(S) \cap f(T)$ is not a subset of $f(S \cap T)$. There there is an element b in $f(S) \cap f(T)$ such that $b \notin f(S \cap T)$, *i.e.*, $b = f(s)$ for some $s \in S$ and $b = f(t)$ for some $t \in T$, but for all $a \in S \cap T$ we have that $b \ne f(a)$. It follows that neither s nor t can be elements of $S \cap T$. Thus s is in S but not in $S \cap T$, while t is in T but not in $S \cap T$. Therefore s and t are distinct, $s \ne t$. But $f(s) = f(t) = b$. This contradicts that f is one-to-one.

12. Let Z^+ denote all positive integers, *i.e.*, $Z^+ = \{1, 2, 3, \cdots\}$.

(a) Let f be the function from $Z^+ \times Z^+$ to Z^+ given by

$$f(n_1, n_2) \;=\; n_1 + n_2\ .$$

Is f one-to-one? Is f onto? Justify your answers.

(b) Can you describe a function from $Z^+ \times Z^+$ to Z^+ that is one-to-one and onto?

SOLUTION:

(a) f is not one-to-one; for example, $f(1, 2) = f(2, 1)$. Also, f is not onto, since $f(n_1, n_2) \ne 1$, for all n_1, n_2.

(b) Order the elements of $Z^+ \times Z^+$ as follows:

$$\begin{array}{ccccc} (1,1) & (1,2) & (1,3) & (1,4) & \cdots \\ (2,1) & (2,2) & (2,3) & (2,4) & \cdots \\ (3,1) & (3,2) & (3,3) & (3,4) & \cdots \\ (4,1) & (4,2) & (4,3) & (4,4) & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

Now "count" the elements of $Z^+ \times Z^+$ "anti-diagonally", that is,

$$
\begin{array}{c}
(1,1) \mapsto 1 \\
(1,2) \mapsto 2 \qquad (2,1) \mapsto 3 \\
(1,3) \mapsto 4 \qquad (2,2) \mapsto 5 \qquad (3,1) \mapsto 6 \\
(1,4) \mapsto 7 \qquad (2,3) \mapsto 8 \qquad (3,2) \mapsto 9 \qquad (4,1) \mapsto 10
\end{array}
$$

and so on. By construction this defines a function from $Z^+ \times Z^+$ to Z^+ that is one-to-one and onto.