CONCORDIA UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

COMP 232: MATHEMATICS FOR COMPUTER SCIENCE
FALL 2015

ASSIGNMENT 3: SOLUTIONS

PROBLEM 1.

Let A and B be sets. Prove that $A \subseteq B$ if and only if $P(A) \subseteq P(B)$.

SOLUTION.

LHS $\Rightarrow$ RHS.

Let $A \subseteq B$, and let $S \in P(A)$. Then, $S \subseteq A$ and $A \subseteq B$, and so $S \subseteq B$, that is, $S \in P(B)$. Therefore, $A \subseteq B \Longrightarrow P(A) \subseteq P(B)$.

RHS $\Rightarrow$ LHS.

Let $P(A) \subseteq P(B)$, and let $a \in A$. Then, $\{a\} \subseteq A$, that is, $\{a\} \in P(A)$. This, in turn, means that $\{a\} \in P(B)$, and so $\{a\} \subseteq B$ or that $a \in B$. Therefore, $P(A) \subseteq P(B) \Longrightarrow A \subseteq B$.

Note. This result is simply saying that A is a subset of B if and only if every subset of A is also a subset of B.

PROBLEM 2.

Let A, B, C, and D be sets. Prove or disprove the following:

$$(A \cap B) \cup (C \cap D) = (A \cap D) \cup (C \cap B).$$

SOLUTION.

This can be disproven by a counterexample. Let $A = \{1\}$, $B = \{2\}$, $C = \{2\}$, and $D = \{1\}$. Then, LHS = $\varnothing$, however, RHS = $\{1, 2\}$.

PROBLEM 3.

Give an example of two uncountable sets A and B such that $A - B$ is

(a) Countably Infinite.
(b) Uncountable.

SOLUTION.

In each case, let A be the set of real numbers.

(a) Let B be the set of real numbers that are not positive integers, that is, $B = A - \mathbf{Z}^+$. Then, $A - B = \mathbf{Z}^+$, which is countably infinite.

(b) Let B be the set of positive real numbers. Then, $A - B$ is the set of negative real numbers and 0, which is uncountable.

PROBLEM 4.

Prove that $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor$.

SOLUTION.

Let $x = n + \varepsilon$, $0 \le \varepsilon < 1$. Then,

LHS $= \lfloor 3n + 3\varepsilon \rfloor = 3n + \lfloor 3\varepsilon \rfloor$, and
RHS $= \lfloor n + \varepsilon \rfloor + \lfloor n + \varepsilon + 1/3 \rfloor + \lfloor n + \varepsilon + 2/3 \rfloor = 3n + \lfloor \varepsilon + 1/3 \rfloor + \lfloor \varepsilon + 2/3 \rfloor$.

Now, depending on the range of values of ε, there are three exhaustive cases:

Case 1: $0 \le \varepsilon < 1/3$.

LHS $= 3n$, since $0 \le 3\varepsilon < 1$, and
RHS $= 3n$, since $1/3 \le \varepsilon + 1/3 < 2/3$ and $2/3 \le \varepsilon + 2/3 < 1$.

Case 2: $1/3 \le \varepsilon < 2/3$.

LHS $= 3n + 1$, since $1 \le 3\varepsilon < 2$, and
RHS $= 3n + 1$, since $2/3 \le \varepsilon + 1/3 < 1$ and $1 \le \varepsilon + 2/3 < 4/3$.

Case 3: $2/3 \le \varepsilon < 1/3$.

LHS $= 3n + 2$, since $2 \le 3\varepsilon < 3$, and
RHS $= 3n + 2$, since $1 \le \varepsilon + 1/3 < 4/3$ and $4/3 \le \varepsilon + 2/3 < 5/3$.

Therefore, $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor$.

PROBLEM 5.

(a) Give an example of a function from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ that is neither one-to-one nor onto.

(b) Let $g : A \rightarrow B$ and $f : B \rightarrow C$ be functions. Let $f \circ g$ be onto. Are both f and g necessarily onto?
(c) Let f be a function from **R** to **R** defined by $f(x) = x^2$. Find $f^{-1}(\{x \mid 0 < x < 1\})$.

SOLUTION.

(a) $\lfloor (x + 4)/2 \rfloor$. It is not one-to-one because both $x = 2$ and $x = 3$ map to 3. It is not onto because there is no preimage of 1.

(b) No. Let $A = \{a_1\}$, $B = \{b_1, b_2\}$, and $C = \{c_1\}$, and define $g(a_1) = b_1$, $f(b_1) = c_1$, $f(b_2) = c_1$. Then, $f \circ g$ and f are onto, but g is not.

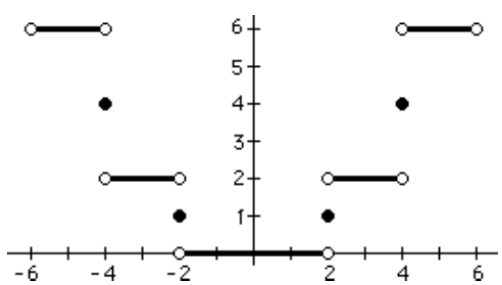
(c) In order for x^2 to be strictly between 0 and 1, x needs to be either strictly between 0 and 1 or strictly between −1 and 0. Therefore, the solution is $\{x \mid (-1 < x < 0) \vee (0 < x < 1)\}$.

PROBLEM 6.

Draw the graph of $\lceil x/2 \rceil \cdot \lfloor x/2 \rfloor$.

SOLUTION.

The underlying shape is the parabola, $y = x^2/4$. However, because of the step functions, the graph is broken into steps, as shown below:



PROBLEM 7.

Let a and b be integers, and m be a positive integer. Prove that

$$ab \equiv [\ (a \text{ (mod m)}) \cdot (b \text{ (mod m)})\ ] \text{ (mod m)}.$$

SOLUTION.

Let $c = a$ (mod m) and $d = b$ (mod m).

Then, a = pm + c and b = qm + d, for some integers p and q.

Now, $ab - cd = (\text{pm} + c)(\text{qm} + d) - cd = \text{pqm}^2 + d\text{pm} + c\text{qm} + cd - cd = \text{m}(\text{pqm} + d\text{p} + c\text{q})$.

In other words, $\text{m} \mid (ab - cd)$. Therefore, $ab \equiv cd \pmod{\text{m}}$.

PROBLEM 8.

Prove that $a^3 \equiv a \pmod 3$ for every positive integer a.

SOLUTION.

There are three exhaustive cases, depending on whether a is a multiple of 3 or not:

Case 1: $a = 3\text{k}$.

Then, $a^3 = 27\text{k}^3 = 3(9\text{k}^2)$. Therefore, $a^3 - a = 3(9\text{k}^2) - 3\text{k} = 3(9\text{k}^2 - \text{k})$.

Case 2: $a = 3\text{k} + 1$.

Then, $a^3 = 27\text{k}^3 + 27\text{k}^2 + 9\text{k} + 1 = 3(9\text{k}^3 + 9\text{k}^2 + 3\text{k}) + 1$. Therefore, $a^3 - a = [3(9\text{k}^3 + 9\text{k}^2 + 3\text{k}) + 1] - [3\text{k} + 1] = 3(9\text{k}^3 + 9\text{k}^2 + 2\text{k})$.

Case 3: $a = 3\text{k} + 2$.

Then, $a^3 = 27\text{k}^3 + 54\text{k}^2 + 36\text{k} + 8 = 3(9\text{k}^3 + 18\text{k}^2 + 12\text{k} + 2) + 2$. Therefore, $a^3 - a = [3(9\text{k}^3 + 18\text{k}^2 + 12\text{k} + 2) + 2] - [3\text{k} + 2] = 3(9\text{k}^3 + 18\text{k}^2 + 11\text{k})$.

In each case, $a^3 \equiv a \pmod 3$.

Note. The problem could also be solved by mathematical induction, that is, by showing that $3 \mid (a^3 - a)$, for every positive integer a.

PROBLEM 9.

Prove that if p is a prime number greater than 3, then $p^2 = 6\text{k} + 1$, for some integer k.

SOLUTION.

If p is a prime number greater than 3, then $p \pmod 6$ cannot be 0, 2, or 4, as that would mean p is even, and $p \pmod 6$ cannot be 3 as that would mean p is a multiple of 3.

The only two remaining cases are $p \pmod 6 = 1$ and $p \pmod 6 = 5$.

Case 1: $p \pmod 6 = 1$.

Then, $p = 6\text{j} + 1$, for some integer j. This means

$p^2 = 36j^2 + 12j + 1 = 6(6j^2 + 2j) + 1 = 6k + 1$, where $k = 6j^2 + 2j$.

Case 2: $p \pmod 6 = 5$.

Then, $p = 6j + 5$, for some integer j. This means

$p^2 = 36j^2 + 60j + 25 = 6(6j^2 + 10j + 4) + 1 = 6k + 1$, where $k = 6j^2 + 10j + 4$.

PROBLEM 10.

Let a, b, and d be integers such that $d \geq 2$ and $a \equiv b \pmod d$. Prove that $\gcd(a, d) = \gcd(b, d)$.

SOLUTION.

From $a \equiv b \pmod d$, it follows that $b = a + sd$, for some integer s. Now, if d is a common divisor of a and d, then it divides the RHS of this equation, and so it also divides b.

The previous equation can be rewritten as $a = b - sd$. Then, by similar reasoning, it follows that every common divisor of b and d is also a divisor of a.

This shows that $(d \mid a \text{ and } d \mid d) \Longrightarrow (d \mid b)$, and $(d \mid b \text{ and } d \mid d) \Longrightarrow (d \mid a)$, which is logically equivalent to $(d \mid a) \Longrightarrow (d \mid b)$ and $(d \mid b) \Longrightarrow (d \mid a)$. Thus, the set of common divisors of a and d is equal to the set of common divisors of b and d, and so $\gcd(a, d) = \gcd(b, d)$.