Problem Set 3 Solutions

Problem 3-1. We first show that we can put g gallons into the receptacle only if $c|g$. We prove this by induction on the number of operations. Let $P(n)$ be " after n operations buckets A, B and the receptacle contain a number of gallons of water which is divisible by $c = gcd(a, b)$.
BASE CASE: $P(1)$ is clearly true since the containers contain either a or b gallons and $c|a$ and $c|b$.
INDUCTIVE STEP: Assume $P(n)$ is true. Consider $(n+1)$ operations. At the end of the first n operations, by the inductive hypothesis, all containers contain a number of gallons divisible by c. For the $(n+1)$th operation we consider the different cases:

- fill bucket A or bucket B from either the hose or the receptacle - the proposition holds for this case, trivially.
- empty bucket A or bucket B to the drain or the receptacle - the proposition holds for this case, trivially.
- pour from A to B until either A is empty or B is full - by the inductive hypothesis since A and B each contained a number divisible by c, they continue to do so after this operation.
- pour from B to A until either B is empty or A is full - identical to the previous case.

This shows that $P(n+1)$ is true. Hence $P(n)$ is true for all natural numbers n.

We now show that if $c|g$ then we can put g gallons into the receptacle. Let $g = kc$. Now by Theorem 7.5 of Handout 13, Notes 4, we have that $c = ax + by$ for some integers x and y, both of which cannot be negative. Without loss of generality let x be positive. Then fill bucket A and empty into the receptacle kx times. Then since y must be negative fill bucket B from the receptacle and empty into the drain $|ky|$ times. Note that this leaves us with the desired $g = kc$ gallons in the receptacle.

Note that $3 \cdot 49 - 133 = 14$. So fill the receptacle using the 49 ounce bucket three times and empty it once using the 133 ounce bucket. This will leave exactly 14 gallons in the receptacle.

Problem 3-2. **(a)** There are many right answers. Here are a pair of keys that work: $d = 21$ and $e = 6061$.

(b) "MIT"$= 26^2 * 12 + 26 * 8 + 19 = 8339$. Encryption: $8339^{6061} = 22873 \bmod 25777$. Hence the encrypted version of "MIT" $= 22873$. Decryption: $22873^{21} = 8339 \bmod 25777$.

(c) "YOU"$= 16608$. But $gcd(16608, 25777) = 173$ and hence security would be compromised. 173 would continue to be a factor of the encrypted version of "YOU" so that anyone listening to the encrypted version would be able to use Euclid's algorithm on $n = pq$ and M^e to obtain a factor p. Having the factors of n it is a simple matter to reconstruct d from e and break the code.

Problem 3-3. Let m and n be any two natural numbers. Let M be the set of multiples of m and N the multiples of n. Consider $M \cap N$. It is nonempty since it contains mn. By the well-ordering principle it contains a least element which is the least common multiple of m and n. Hence every pair of natural numbers has a least common multiple.

Let $a = \prod_i p_i^{\alpha_i}$ and $b = \prod_i p_i^{\beta_i}$ where $p_1, p_2 \ldots$ are the primes in increasing order. Following Theorem 7.12 in Handout 13, Notes 4, it was shown that $gcd(a,b) = \prod_i p_i^{\min(\alpha_i,\beta_i)}$. By an identical argument it can be seen that $lcm(a,b) = \prod_i p_i^{\max(\alpha_i,\beta_i)}$. Now, from the fact that for any α and β, $\alpha + \beta = \max(\alpha,\beta) + \min(\alpha,\beta)$, it follows that $a \cdot b = gcd(a,b) \cdot lcm(a,b)$.

Problem 3-4. **(a)** We first show that $A \subset A \cap (A \cup B)$. Consider any $a \in A$. Since $a \in A$ and $a \in (A \cup B)$ it follows that $a \in A \cap (A \cup B)$. This proves that $A \subset A \cap (A \cup B)$.

We now show that $A \cap (A \cup B) \subset A$. Consider any $a \in A \cap (A \cup B)$. It must be the case that $a \in A$. Hence $A \cap (A \cup B) \subset A$.

From the above we get that $A \cap (A \cup B) = A$.

(b) We first show that $A \subset B$. Consider any $a \in A$. Then $\{a\} \in \mathcal{P}(A)$. But $\mathcal{P}(A) = \mathcal{P}(B)$. Hence $\{a\} \in \mathcal{P}(B)$. This implies that $a \in B$. This proves that $A \subset B$.

The argument to show that $B \subset A$ follows from symmetry. Hence $A = B$.

(c) That the theorem is plainly false can be seen from the case of the empty relation which is both symmetric and transitive but not reflexive. The error in the proof lies in the statement " Take an element $b \in A$ such that $(a,b) \in R$." Such an element may not exist.

Problem 3-5. **(a)** We first show that $(A \times B) \cap (B \times A) \subset (A \cap B) \times (A \cap B)$. Consider any $(c,d) \in (A \times B) \cap (B \times A)$. Since $(c,d) \in (A \times B)$ this implies that $c \in A$ and $d \in B$. Similarly, since $(c,d) \in (B \times A)$ this implies that $c \in B$ and

$d \in A$. Hence $c, d \in (A \cap B)$. Thus $(c, d) \in (A \cap B) \times (A \cap B)$. This proves that $(A \times B) \cap (B \times A) \subset (A \cap B) \times (A \cap B)$.

We now show that $(A \cap B) \times (A \cap B) \subset (A \times B) \cap (B \times A)$. Consider any $(c, d) \in (A \cap B) \times (A \cap B)$. Then $(c, d) \in (A \cap B)$. Hence $(c, d) \in (A \times B)$ and $(c, d) \in (B \times A)$. Hence $(c, d) \in (A \times B) \cap (B \times A)$. This proves that $(A \cap B) \times (A \cap B) \subset (A \times B) \cap (B \times A)$.

From the above we get that $(A \times B) \cap (B \times A) = (A \cap B) \times (A \cap B)$

(b) Consider any $(c, d) \in (A \times B) \cup (B \times A)$. Then $(c, d) \in (A \times B)$ or $(c, d) \in (B \times A)$. That is $\underline{c \in A \text{ and } d \in B}$ or $\underline{c \in B \text{ and } d \in A}$. In both cases $(c, d) \in (A \cup B) \times (A \cup B)$. Thus $(c, d) \in (A \times B) \cup (B \times A)$. This proves that $(A \times B) \cup (B \times A) \subseteq (A \cup B) \times (A \cup B)$

(c) Let $A = \{a\}$ and $B = \{b\}$. Then $(a, a) \in (A \cup B) \times (A \cup B)$ but $(a, a) \notin (A \times B) \cup (B \times A)$.

Problem 3-6. Let $P(n)$ be "any set of cardinality n has exactly 2^{n-1} subsets of even size."
BASIS STEP: $P(1)$ is true since any set of cardinality 1 has exactly one even-sized subset - the empty set.
INDUCTIVE STEP: Assume $P(n)$ is true. Consider any set of cardinality $n+1$. Arbitrarily pick one of the elements to be a distinguished element. The collection of all subsets of this set can be partitioned into two groups: those containing the distinguished element and those not containing it.

Now, the first group - the collection of subsets not containing the distinguished element - is identical to the collection of all subsets on the set consisting of the remaining n nondistinguished elements. Hence it contains exactly 2^{n-1} subsets of even size.

Now consider the collection of subsets containing the distinguished element and remove this distinguished element from each subset. We are left with a collection that is identical to the collection of all subsets on the set consisting of the remaining n nondistinguished elements. Since this collection has totally 2^n elements and exactly 2^{n-1} subsets of even size it must also contain exactly 2^{n-1} subsets of odd size. So on adding the distinguished element back in we find that the second group - the collection of subsets containing the distinguished element - contains exactly 2^{n-1} subsets of even size.

Hence any set of cardinality $n + 1$ has exactly $2^{n-1} + 2^{n-1} = 2^n$ subsets of even size. Thus $P(n + 1)$ is true. Hence $P(n)$ is true for all natural numbers n.