CONCORDIA UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

COMP232 MATHEMATICS FOR COMPUTER SCIENCE

ASSIGNMENT 3 FALL 2013

1. Prove each of the following, using proper, well-defined set-theoretic notation:

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

   (b) $(A \cup B) \subseteq C$ if and only if $A \subseteq C$ and $B \subseteq C$.

   SOLUTION:

   (a) :
   $$\begin{aligned} A \cup (B - A) &= \{\, x : \; x \in A \vee (x \in B \wedge x \notin A) \,\} \\ &= \{\, x : \; (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A) \,\} \\ &= \{\, x : \; (x \in A \vee x \in B) \wedge \text{True} \,\} \\ &= \{\, x : \; x \in A \vee x \in B \,\} \;=\; A \cup B \;. \end{aligned}$$

   (b) :

   ($\Leftarrow$) Suppose $(A \subseteq C)$ and $B \subseteq C$, and let $x \in A \cup B$. Then $x \in A$ or $x \in B$.

   If $x \in A$ then $x \in C$, since $A \subseteq C$. Similarly, if $x \in B$ then $x \in C$, since $B \subseteq C$.

   ($\Rightarrow$) We prove the contrapositive: if $A \not\subseteq C$ or $B \not\subseteq C$ then $(A \cup B) \not\subseteq C$.

   Case 1: $A \not\subseteq C$. Then $\exists x \in A - C$. Since x also is in $A \cup B$, it follows that $(A \cup B) \not\subseteq C$.

   Case 2: $B \not\subseteq C$. Similar to case 1.

2. If A and B are sets and $f : A \longrightarrow B$, then for any subset S of A we define

   $$f(S) \;=\; \{b \in B : b = f(a) \text{ for some } a \in S\} \;.$$

   Similarly, for any subset T of B we define the *pre-image* of T as

   $$f^{-1}(T) \;=\; \{a \in A : f(a) \in T\} \;.$$

   Note that $f^{-1}(T)$ is well-defined even if f does not have an inverse !

   Now let $f \;:\; \mathbb{Z} \longrightarrow \mathbb{Z}$ be defined as $f(n) = n^2$. Let S_1 denote the set $\{-2, -1, 0, 1\}$, and let S_2 be the set $\{-1, 0, 1, 2\}$.

   Determine

   $$f(S_1 \cup S_2) \;,\; f(S_1) \cup f(S_2) \;,\; f(S_1 \cap S_2) \;,\; f(S_1) \cap f(S_2) \;,$$

   and

   $$f^{-1}(S_1 \cup S_2) \;,\; f^{-1}(S_1) \cup f^{-1}(S_2) \;,\; f^{-1}(S_1 \cap S_2) \;, \text{ and } f^{-1}(S_1) \cap f^{-1}(S_2) \;.$$

   SOLUTION: Since $S_1 \cup S_2 = \{-2, -1, 0, 1, 2\}$, and $S_1 \cap S_2 = \{-1, 0, 1\}$, we find that

   $f(S_1) \;=\; f(S_2) \;=\; f(S_1) \cup f(S_2) \;=\; f(S_1) \cap f(S_2) \;=\; \{0, 1, 4\}$, while $f(S_1 \cap S_2) = \{0, 1\}$.

   We also find that $f^{-1}(S_1) = f^{-1}(S_2) = \{0, -1, 1\}$, and also

   $f^{-1}(S_1 \cup S_2) \;=\; f^{-1}(S_1) \cup f^{-1}(S_2) \;=\; f^{-1}(S_1 \cap S_2) \;=\; f^{-1}(S_1) \cap f^{-1}(S_2) \;=\; \{0, -1, 1\}$.

3. Let A and B be arbitary sets. Let S_1 and S_2 be arbitrary subsets of A, and let T_1 and T_2 be arbitrary subsets of B. For each of the following state whether it is True or False. If True then give a proof. If False then give a counterexample:

   (a) $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$ (b) $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$

   (c) $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$ (d) $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$

   SOLUTION:

   (a) $b \in f(S_1 \cup S_2) \Leftrightarrow \exists a \in A : a \in (S_1 \cup S_2) \ \wedge \ f(a) = b$
   $\Leftrightarrow \exists a \in A : (a \in S_1 \vee a \in S_2) \ \wedge \ f(a) = b$
   $\Leftrightarrow \exists a \in A : (a \in S_1 \wedge f(a) = b) \ \vee \ (a \in S_2 \wedge f(a) = b)$
   $\Leftrightarrow b \in f(S_1) \ \vee \ b \in f(S_2)$
   $\Leftrightarrow b \in f(S_1) \cup f(S_2)$.

   (b) This identity is not always valid. A counterexample can be found in Problem 2. What is True is that $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$.

   (c) $a \in f^{-1}(T_1 \cup T_2) \Leftrightarrow \exists b \in B : b \in (T_1 \cup T_2) \ \wedge \ f(a) = b$
   $\Leftrightarrow \exists b \in B : (b \in T_1 \vee b \in T_2) \ \wedge \ f(a) = b$
   $\Leftrightarrow \exists b \in B : (b \in T_1 \wedge f(a) = b) \ \vee \ (b \in T_2 \wedge f(a) = b)$
   $\Leftrightarrow a \in f^{-1}(T_1) \ \vee \ a \in f^{-1}(T_2)$
   $\Leftrightarrow a \in f^{-1}(T_1) \cup f^{-1}(T_2)$.

   (d) $a \in f^{-1}(T_1 \cap T_2) \Leftrightarrow \exists b \in B : b \in (T_1 \cap T_2) \ \wedge \ f(a) = b$
   $\Leftrightarrow \exists b \in B : b \in T_1 \ \wedge \ b \in T_2 \ \wedge \ f(a) = b$
   $\Leftrightarrow \exists b \in B : b \in T_1 \wedge f(a) = b \ \wedge \ b \in T_2 \wedge f(a) = b$
   $\Leftrightarrow a \in f^{-1}(T_1) \ \wedge \ a \in f^{-1}(T_2)$
   $\Leftrightarrow a \in f^{-1}(T_1) \cap f^{-1}(T_2)$.

4. Let $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ 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: f is one-to-one: Suppose $f(m_1, n_1) = f(m_2, n_2)$. Then $3m_1+7n_1 = 3m_2+7n_2$ and $2m_1 + 5n_1 = 2m_2 + 5n_2$. Multiplying the first of these equations by 2 and the second by 3, and subtracting the former from the latter, gives $n_1 = n_2$. Substituting $n_1 = n_2$ in $3m_1 + 7n_1 = 3m_2 + 7n_2$ gives $3m_1 = 3m_2$, so that also $m_1 = m_2$. Hence f is one-to-one.

   f is also onto: Let $(k, \ell) \in \mathbb{Z}^2$. We must show that there exists $(m, n) \in \mathbb{Z}^2$ so that $f(m, n) = (k, \ell)$. This gives the equations $3m + 7n = k$ and $2m + 5n = \ell$. Multiplying the first of these equations by 2 and the second by 3, and subtracting the former from the latter now gives $n = 3\ell - 2k$. Substituting this in $3m + 7n = k$ gives $3m + 7(3\ell - 2k) = k$, from which it follows that $m = 5k - 7\ell$. Since both m and n are indeed integers, it follows that f is onto.

   Given that f has been shown to be one-to-one, the above proof that f is onto also provides the formula for the inverse, namely, $f^{-1}(k, \ell) = (5k - 7\ell, -2k + 3\ell)$.

5. Does there exist a function $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ that is one-to-one and onto, and hence invertible? If such a function exists then give a clear description of it. If such a function does not exist then explain why not.

   SOLUTION: The set $\mathbb{Z}^2$ is indeed countably infinite. An invertible function $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ can be constructed as follows:

$$\begin{array}{llllllllll} (0,0) & \mapsto 0, & (1,0) & \mapsto -1, & (1,1) & \mapsto 1, & (0,1) & \mapsto -2, & (-1,1) & \mapsto 2, \\ (-1,0) & \mapsto -3, & (-1,-1) & \mapsto 3, & (0,-1) & \mapsto -4, & (1,-1) & \mapsto 4, & (2,-1) & \mapsto -5, \\ (2,0) & \mapsto 5, & (2,1) & \mapsto -6, & (2,2) & \mapsto 6, & (1,2) & \mapsto -7, & (0,2) & \mapsto 7, \\ (-1,2) & \mapsto -8, & (-2,2) & \mapsto 8, & (-2,1) & \mapsto -9, & (-2,0) & \mapsto 9, & \text{etcetera.} & \end{array}$$

   By construction this function is one-to-one. It is also onto, because the above scheme will reach any element $m \in \mathbb{Z}$ in a finite number of steps.

6. Let $S = \{0, 1, 2, 3, \cdots, 99\}$. For each of the following functions $f : S \longrightarrow S$, determine whether it is one-to-one and onto, by computing its values for all $k \in S$:

$$f(k) = (131k+27) \bmod 100, \quad f(k) = (132k+27) \bmod 100, \quad f(k) = (133k+27) \bmod 100$$

   SOLUTION: A simple calculation on a computer shows that the first and third functions are one-to-one and onto, while the second function is not.

   REMARK: A general result for this type of problem is the following: For $n > 2$, let $S_n = \{0, 1, 2, 3, \cdots, n-1\}$, p a prime number greater than n, and $s \in S_n$. Then the function $f : S_n \longrightarrow S_n$ given by $f(k) = (pk + s) \bmod n$ is one-to-one and onto. PROOF: Suppose $f(k_1) = f(k_2)$. Then $(pk_1 + s) \bmod n = (pk_2 + s) \bmod n$, from which it follows that $n|((pk_1 + s) - (pk_2 + s))$, that is, $n|p(k_1 - k_2)$. Clearly, since $n > p$, p is not divisible by n. Moreover, the only factor of n that divides p is 1, because p is prime. Hence we must have that $n|(k_1 - k_2)$. However, since $k_1, k_2 \in S_n$, we see that $-(n-1) \leq k_1 - k_2 \leq n-1$. The only value in this range that is divisible by n is 0, that is, $k_1 - k_2 = 0$. Thus $k_1 = k_2$, so that f is one-to-one. Since f is an injection from a finite set into itself it is therefore also onto, and hence invertible.

   In the preceding problem we had $p = 131, 132, 133$, respectively, and $s = 27$, where 131 is prime, but 132 and 133 are not prime. In agreement with the result proved above, the case $p = 131$ gives an invertible function. Note that the case $p = 133$, which is not prime, also gives an invertible function. This shows that the converse of the result proved above is not valid: if f is invertible then p is not necessarily prime.

7. Use the Euclidean algorithm to determine whether or not the years 1892 and 2013 are relatively prime.

   SOLUTION:

   $\gcd(2013, 1892) = \gcd(1892, 2013 \bmod 1892) = \gcd(1892, 121) = \gcd(121, 1892 \bmod 121) = \gcd(121, 77) = \gcd(77, 121 \bmod 77) = \gcd(77, 44) = \gcd(44, 77 \bmod 44) = \gcd(44, 33) = \gcd(33, 44 \bmod 33) = \gcd(33, 11) = \gcd(11, 33 \bmod 11) = \gcd(11, 0) = 11$. Thus 1812 and 2013 are not relatively prime.

8. When an integer n is divided by 6, the remainder is 5. What are the possible values of the remainder when $9n$ is divided by 8 ?

   SOLUTION: We have $n = 6k + 5$, so that $9n = 9 \cdot 6k + 9 \cdot 5 = 54k + 45$. Thus $9n \bmod 8 = (54k+45) \bmod 8 = ((6 \cdot 8+6)k+5 \cdot 8+5) \bmod 8 = (6k+5) \bmod 8$. A simple calculation shows that for $k = 0, 1, 2, \cdots, 7$, the values of $(6k + 5) \bmod 8$ are $5, 3, 1, 7, 5, 3, 1, 7$, respectively. Thus, depending on n, the value of $9n \bmod 8$ can be equal to 1, 3, 5, and 7.

9. Find all integer solutions of $2n \equiv 13 (\text{mod } 19)$.

   SOLUTION: We have $2n = 19k+13$ for some integer k. Thus $19k+13$ must be even, so that k must be odd, that is, $k = 2k_1+1$, for some integer k_1. This gives $2n = 19(2k_1+1)+13 = 38k_1 + 32$, from which $n = 19k_1 + 16$, that is, $n \equiv 16 (\text{mod } 19)$.

10. Use a proof by cases to show that for $m, n \in \mathbb{Z}^+$, $\gcd(m + n, mn) - \gcd(m, n)$ is even.

    PROOF: If both m and n are even then both are divisible by 2, and hence both $m+n$ and mn are divisible by 2. Thus the greatest common divisor of $m + n$ and mn must contain the factor 2, *i.e.*, it must be even. Similarly, $\gcd(m, n)$ is even. Hence $\gcd(m + n, mn) - \gcd(m, n)$ is even.

    If both m and n are odd then $m + n$ is even, while mn is odd. Thus $\gcd(m + n, mn)$ cannot contain the factor 2, *i.e.*, it must be odd. Similarly, $\gcd(m, n)$ is odd. Hence $\gcd(m + n, mn) - \gcd(m, n)$ is even.

    If m is odd and n even then $m + n$ is odd, while mn is even. Thus $\gcd(m + n, mn)$ cannot contain the factor 2, *i.e.*, it must be odd. Similarly, $\gcd(m, n)$ is odd. Hence $\gcd(m + n, mn) - \gcd(m, n)$ is even.

    The case m is even and n odd follows similarly.