

Math 74 Homework 10: Selected Solutions

November 10, 2008

1. Let X be a set, and suppose that X is not finite. Using an inductive definition, show that there is an injective function $f : \mathbb{N} \rightarrow X$.

Solution: We define f inductively as follows: since X is not finite, it is not empty, so there exists some $x_0 \in X$. Let $f(0) = x_0$. Now, suppose that we have defined $f(0), f(1), \dots, f(n)$, and that $f(i) \neq f(j)$ for $i, j \in A_{n+1}$, $i \neq j$. If $f : A_{n+1} \rightarrow X$ were surjective, then X would be finite; hence f as defined so far is not surjective, i.e. there is an $x_{n+1} \in X$ such that $x_{n+1} \neq f(i)$ for all $i \in A_{n+1}$. Define $f(n+1) = x_{n+1}$. We still have that $f(i) \neq f(j)$ for $i, j \in A_{n+2}$, $i \neq j$.

Hence by induction we get a function $f : \mathbb{N} \rightarrow X$. We want to show that f is injective. Suppose $f(i) = f(j)$ for some $i, j \in \mathbb{N}$. Without loss of generality, $i \geq j$, so $i, j \in A_{i+1}$. But we know that $f|_{A_{i+1}}$ is injective by construction, hence $i = j$. Thus f is injective.

2. (Equivalence Relations and Partitions are in Bijective Correspondence)
 - (a) Let X be a set, and let $P \subseteq P(X)$ be a partition of X . Define a relation R_P on X by aR_Pb iff there exists an $A \in P$ such that $a \in A$ and $b \in A$. Show that R_P is an equivalence relation.
 - (b) Now let R be an arbitrary equivalence relation on X . We showed in class that the set $X/R \subseteq P(X)$ is a partition of X . Show that the functions $R \mapsto X/R$ and $P \mapsto R_P$ are inverse bijections between the set of equivalence relations on X and the set of partitions of X .

Note: This exercise is extremely important; this correspondence between partitions and equivalence relations is very useful, and

should form a large part of the basis of your understanding of equivalence relations.

Solution to a): Reflexivity: Let $x \in X$. By the definition of a partition, there exists an $A \in P$ such that $x \in A$. Hence xR_Px .

Symmetry: Suppose xR_Py . Then there exists an $A \in P$ such that $x \in A$ and $y \in A$. Hence $y \in A$ and $x \in A$, so yR_Px .

Transitivity: Suppose xR_Py and yR_Pz . Then there exists an $A \in P$ such that $x \in A$ and $y \in A$, and there exists a $B \in P$ such that $y \in B$ and $z \in B$. Now, $y \in A \cap B$, so $A \cap B \neq \emptyset$. Hence by the definition of a partition, we have $A = B$. Hence $x \in A$ and $z \in A$, so xR_Pz .

Solution to b): Let R be an arbitrary equivalence relation and let P be an arbitrary partition. We need to show that $X/R_P = P$ and $R_{X/R} = R$.

Let's show that $X/R_P = P$ first. To show this, I claim that it suffices to show that if $A \in P$ then $A \in X/R_P$. Indeed, this will show that $P \subseteq X/R_P$. But suppose for contradiction that there were some $B \in X/R_P$ such that $B \notin P$. Then there exists a $b \in B \subseteq X$, and since P is a partition, there exists an $A \in P$ such that $b \in A$. But by the assumption that $P \subseteq X/R_P$, we have that $A \in X/R_P$. Now, $b \in A \cap B$, hence $A = B$. This contradicts the assumption that $B \notin P$.

So, let's show that if $A \in P$ then $A \in X/R_P$. Let $A \in P$ be arbitrary, and choose an $a \in A$. Then

$$\begin{aligned} [a]_{R_P} &= \{b \in X \mid aR_Pb\} \\ &= \{b \in X \mid \exists B \in P \text{ such that } a \in B \text{ and } b \in B\}. \end{aligned}$$

Now, for $B \in P$, we have $a \in B$ iff $B = A$ by the definition of a partition. Hence we can rewrite the above set as

$$\{b \in X \mid b \in A\},$$

which is just A . Hence $A = [a]_{R_P} \in X/R_P$, as desired.

Now let's show that $R_{X/R} = R$. Let $a, b \in X$ be arbitrary. Suppose $aR_{X/R}b$. Then by definition, there exists an $A \in X/R$

such that $a \in A$ and $b \in A$, i.e. a and b have the same R -equivalence class, i.e. aRb . On the other hand, suppose aRb . Then $[a]_R = [b]_R$, so $a \in [a]_R$ and $b \in [a]_R$, hence $aR_{X/R}b$.

3. Let X be a set, let \leq be a partial order relation on X , and let $Y \subseteq X$. Show that if a least upper bound for Y exists, then it is unique. Do the same for greatest lower bounds for Y .

Solution: Let a and b be two least upper bounds for Y . Then b is in particular an upper bound, so since a is a least upper bound, we have $a \leq b$. In the same way, we have $b \leq a$. By the anti-symmetry of \leq , we have $a = b$, as desired.

4. Let $a, b \in \mathbb{N} \setminus \{0\}$. Let $p_1 < p_2 < \dots < p_n \in \mathbb{N}$ be all of the prime numbers appearing in the prime factorizations of either a or b . Then there exist unique numbers $r_1, r_2, \dots, r_n, s_1, s_2, \dots, s_n \in \mathbb{N}$ such that

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_n^{r_n} \quad \text{and} \quad b = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_n^{s_n}.$$

- (a) Show that a divides b if and only if $r_i \leq s_i$ for all $i \in \{1, \dots, n\}$.
 (b) For each $i \in \{1, \dots, n\}$, let $\min(r_i, s_i)$ denote the smaller of r_i and s_i (so $\min(1, 2) = 1$, for example). Show that

$$\gcd(a, b) = p_1^{\min(r_1, s_1)} \cdot p_2^{\min(r_2, s_2)} \cdot \dots \cdot p_n^{\min(r_n, s_n)}.$$

- (c) Calculate the prime factorizations of 38700 and 32760. Use part (b) to calculate $\gcd(38700, 32760)$.

Solution to a): Suppose $r_i \leq s_i$ for all i . Let $q = a_1^{s_1 - r_1} \cdot a_2^{s_2 - r_2} \cdot \dots \cdot a_n^{s_n - r_n} \in \mathbb{N}$. Then $aq = b$, so $a \mid b$.

On the other hand, suppose $r_i > s_i$ for some i . Let $q \in \mathbb{N} \setminus \{0\}$ be arbitrary. Now, if $p \mid q$ for some p which does not divide b , then p divides aq , so $aq \neq b$. On the other hand, suppose that the only primes dividing q also divide b . Then we can write

$$q = p_1^{t_1} \cdot p_2^{t_2} \cdot \dots \cdot p_n^{t_n}$$

for some $t_1, \dots, t_n \in \mathbb{N}$. Then we have:

$$aq = p_1^{t_1 + r_1} \cdot p_2^{t_2 + r_2} \cdot \dots \cdot p_n^{t_n + r_n}.$$

This is the unique factorization of aq once we remove those primes with exponent 0. In particular, we see that $aq \neq b$, since the power of p_i in the prime factorization of aq is $r_i + t_i > s_i$, and s_i is the power of p_i in the prime factorization of b . Thus a does not divide b .

Solution to b): Let

$$d = p_1^{\min(r_1, s_1)} \cdot p_2^{\min(r_2, s_2)} \cdots p_n^{\min(r_n, s_n)}.$$

Since $\min(r_i, s_i) \leq r_i$ and $\min(r_i, s_i) \leq s_i$ for all i , we have by (a) that $d \mid a$ and $d \mid b$. On the other hand, if $c \mid a$ and $c \mid b$, then any prime which divides c must divide both a and b , hence in particular the only primes appearing in the prime factorization of c are p_1, \dots, p_n . Write

$$c = p_1^{t_1} \cdot p_2^{t_2} \cdots p_n^{t_n}.$$

By (a) and the assumption that $c \mid a$ and $c \mid b$, we have that $t_i \leq r_i$ and $t_i \leq s_i$ for all i . Hence $t_i \leq \min(r_i, s_i)$ for all i . Thus $c \mid d$, again by (a).

Solution to c) $38700 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 43$. $32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. By (b) we have

$$\gcd(38700, 32760) = 2^2 \cdot 3^2 \cdot 5 = 180.$$

5. Find an inverse to 8 mod 45. Use this to find a solution to the equation $8x = 13 \pmod{45}$.

Solution: We find the inverse to 8 by guess-and-check; there *is* an algorithm for this (called the extended Euclidean algorithm). You can read about it in Eccles.

We calculate: $8 \cdot 17 = 136 = 1 + 3 \cdot 45$, hence $8 \cdot 17 \equiv 1 \pmod{45}$. Hence 17 is an inverse to 8 mod 45. A solution to the given equation is then $x = 17 \cdot 13$.

6. Show that the equation $x^6 + 9x^2 + 1 = 0$ has no integer solutions.

Solution: If the given equation had a solution, c , then we would have that $c^6 + 9c^2 + 1 \equiv 0 \pmod{3}$. Now, $9 \equiv 0 \pmod{3}$, so equivalently we would have $c^6 + 1 \equiv 0 \pmod{3}$. Now, either $c \equiv 0, 1$ or $2 \pmod{3}$. Plugging in 0, 1, and 2 into $c^6 + 1$, we get back $1 \pmod{3}$, $2 \pmod{3}$, and $2 \pmod{3}$, respectively. None of these are $0 \pmod{3}$, so the equation has no solutions.