

Math 74 Midterm 2 Practice Problems: Selected Solutions

November 10, 2008

Easier Problems

- Let X be a set, and let $\text{Rel}(X)$ be the set of relations on X . If $|X| = n$, calculate $|\text{Rel}(X)|$.

Solution: Since a relation on X is the same thing as a subset of $X \times X$, we have $\text{Rel}(X) = \mathcal{P}(X \times X)$. Now, $|X \times X| = n^2$, and so $|\text{Rel}(X)| = |\mathcal{P}(X \times X)| = 2^{n^2}$.

- Find all equivalence relations on the set $X = \{0, 1, 2, 3\}$. For each equivalence relation \sim on X , calculate $|X/\sim|$.

Solution: We use the fact that equivalence relations on X are in bijective correspondence with partitions on X (see HW 10). The partitions on X are easy to write down. They are:

$$\begin{array}{lll}
 \{\{1\}, \{2\}, \{3\}, \{4\}\} & \{\{1, 2\}, \{3\}, \{4\}\} & \{\{1, 3\}, \{2\}, \{4\}\} \\
 \{\{1, 4\}, \{2\}, \{3\}\} & \{\{1\}, \{2, 3\}, \{4\}\} & \{\{1\}, \{2, 4\}, \{3\}\} \\
 \{\{1\}, \{2\}, \{3, 4\}\} & \{\{1, 2\}, \{3, 4\}\} & \{\{1, 3\}, \{2, 4\}\} \\
 \{\{1, 4\}, \{2, 3\}\} & \{\{1, 2, 3\}, \{4\}\} & \{\{1, 2, 4\}, \{3\}\} \\
 \{\{1, 3, 4\}, \{2\}\} & \{\{1\}, \{2, 3, 4\}\} & \{1, 2, 3, 4\}.
 \end{array}$$

Hence there are 15 equivalence relations on X . The partitions above are precisely the description of X/\sim for each of the equivalence relations \sim .

- Let $n, m \in \mathbb{N} \setminus \{0\}$ such that $n \mid m$.
 - Show that if $a \equiv b \pmod{m}$ then $a \equiv b \pmod{n}$. Give an example that shows that the converse is false.

- (b) Show that part (a) implies that the function $f : \mathbb{Z}/\sim_m \rightarrow \mathbb{Z}/\sim_n$ defined by $f([a]_m) = [a]_n$ is well-defined.
- (c) Use this to show that the equation

$$3x^2 + 3x + 1 \equiv 0 \pmod{59706831}$$

has no solution.

Solution to a): Suppose $a \equiv b \pmod{m}$. Then $m \mid (a - b)$ and $n \mid m$, so $n \mid (a - b)$, hence $a \equiv b \pmod{n}$. The numbers $a = 0, b = 2, m = 4, n = 2$ are a counterexample to the converse.

Solution to b): Suppose $[a]_m = [b]_m$. Then $a \equiv b \pmod{m}$, hence $a \equiv b \pmod{n}$, so

$$f([a]_m) = [a]_n = [b]_n = f([b]_m).$$

Solution to c): Notice that $3 \mid 59706831$. So if

$$3c^2 + 3c + 1 \equiv 0 \pmod{59706831}$$

for some $c \in \mathbb{Z}$, then by (b) we would have

$$3c^2 + 3c + 1 \equiv 0 \pmod{3}.$$

But $3c^2 + 3c + 1 \equiv 1 \pmod{3} \neq 0 \pmod{3}$.

4. Let X be a set and let d be the discrete metric on X . Show that a sequence (x_n) in X converges if and only if it is eventually constant, i.e. if and only if there exists an $N \in \mathbb{N}$ such that for all $n, m \geq N$ we have $x_n = x_m$.

Solution: Let (x_n) be an eventually constant sequence; then by definition there exists an $N \in \mathbb{N}$ such that for all $n, m \geq N$ we have $x_n = x_m$, so in particular $x_n = x_N$ for all $n \geq N$. Let $\epsilon > 0$ be arbitrary. Then for all $n \geq N$ we have $d(x_n, x_N) = 0 < \epsilon$, hence (x_n) converges to x_N . (Note: this half of the proof is true in *any* metric space.)

Suppose on the other hand that (x_n) converges to some x . Then there exists an $N \in \mathbb{N}$ such that $d(x_n, x) < \frac{1}{2}$ for all $n \geq N$. Hence we have $d(x_n, x_m) \leq d(x_n, x) + d(x, x_m) < \frac{1}{2} + \frac{1}{2} = 1$ for all $n, m \geq N$. But $d(x, y) < 1$ in X iff $x = y$, so we have $x_n = x_m$

for all $n, m \geq N$. (Note: the triangle inequality portion here could be skipped by noting that since (x_n) is convergent, it is Cauchy).

Medium Problems

5. Recall that we showed that the relation R on $\mathbb{N} \setminus \{0\}$ given by aRb iff $a \mid b$ is a partial order relation, and that we defined $\gcd(a, b)$ to be the greatest lower bound of the set $\{a, b\}$ with respect to this relation, and we defined $\text{lcm}(a, b)$ to be the least upper bound of the set $\{a, b\}$ with respect to this relation. Let $a, b \in \mathbb{N} \setminus \{0\}$ be arbitrary.
- (a) Show that a and $b/\gcd(a, b)$ are relatively prime.
 - (b) Show that if $c, d \in \mathbb{N} \setminus \{0\}$ are relatively prime and $c \mid e$ and $d \mid e$, then $cd \mid e$.
 - (c) Show that $\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$.

Solution to a): Sorry! This is false! Counterexample: $a = 5, b = 25$. Then $\gcd(a, b) = 5$, so $b/\gcd(a, b) = 5$, which is not relatively prime to a . It's possible to correct this statement to make it true, but it requires a lot more care. One improvement could have been: show that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime. This is not so hard: there exist $n, m \in \mathbb{Z}$ such that $an + bm = \gcd(a, b)$. Divide both sides by $\gcd(a, b)$, and we get

$$\frac{a}{\gcd(a, b)}n + \frac{b}{\gcd(a, b)}m = 1,$$

so $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime.

Solution to b): Since c and d are relatively prime, there exist $n, m \in \mathbb{Z}$ such that $cn + dm = 1$. Since $c \mid e$ and $d \mid e$, there exist $p, q \in \mathbb{N}$ such that $cp = e = dq$. Hence

$$e = cne + dme = cndq + dmcp = cd(nq + mp)$$

so $cd \mid e$.

Note that it follows that if $\gcd(c, d) = 1$ then $\text{lcm}(c, d) = cd$.

Solution to c): This would be a lot easier if (a) were true. Since it isn't, here's one possible solution; another nice one would be to describe $\text{lcm}(a, b)$ in terms of the prime factorizations of a and b . Note first that if $c \mid a$ and $c \mid b$, then $\text{lcm}(\frac{a}{c}, \frac{b}{c}) = \frac{\text{lcm}(a, b)}{c}$. Indeed, we have that $a \mid \text{lcm}(a, b)$, so $\frac{a}{c} \mid \frac{\text{lcm}(a, b)}{c}$, and similarly $\frac{b}{c} \mid \frac{\text{lcm}(a, b)}{c}$, so $\text{lcm}(\frac{a}{c}, \frac{b}{c}) \mid \frac{\text{lcm}(a, b)}{c}$. On the other hand, $\frac{a}{c} \mid \text{lcm}(\frac{a}{c}, \frac{b}{c})$ and $\frac{b}{c} \mid \text{lcm}(\frac{a}{c}, \frac{b}{c})$. Hence $a \mid c \cdot \text{lcm}(\frac{a}{c}, \frac{b}{c})$ and $b \mid c \cdot \text{lcm}(\frac{a}{c}, \frac{b}{c})$, so $\text{lcm}(a, b) \mid c \cdot \text{lcm}(\frac{a}{c}, \frac{b}{c})$, hence $\frac{\text{lcm}(a, b)}{c} \mid \text{lcm}(\frac{a}{c}, \frac{b}{c})$. Hence $\text{lcm}(\frac{a}{c}, \frac{b}{c}) = \frac{\text{lcm}(a, b)}{c}$. Hence we have that

$$\text{lcm}(a/\text{gcd}(a, b), b/\text{gcd}(a, b)) = \text{lcm}(a, b)/\text{gcd}(a, b).$$

Since $a/\text{gcd}(a, b)$ and $b/\text{gcd}(a, b)$ are relatively prime, it follows from (b) that

$$\text{lcm}(a/\text{gcd}(a, b), b/\text{gcd}(a, b)) = \frac{ab}{\text{gcd}(a, b)^2}.$$

Putting this together and multiplying by $\text{gcd}(a, b)$ gives

$$\text{lcm}(a, b) = \frac{ab}{\text{gcd}(a, b)}.$$

6. Let $a, b \in \mathbb{N} \setminus \{0\}$. Here are two possible definitions of the least common multiple of a and b :

Definition 1: The *least common multiple* of a and b is smallest number $c \in \mathbb{N} \setminus \{0\}$ such that $a \mid c$ and $b \mid c$.

Definition 2: The *least common multiple* of a and b is a natural number $e \in \mathbb{N} \setminus \{0\}$ such that:

- (a) $a \mid e$ and $b \mid e$
- (b) For all $c \in \mathbb{N} \setminus \{0\}$, if $a \mid c$ and $b \mid c$, then $e \mid c$.

Show that these two definitions agree, i.e. they define the same number.

Solution: It's not even clear that the number in Definition 2 *exists*. We'll show it exists by showing that it is equal to the number defined in Definition 1. Let d be the number in Definition 1 (which exists by well-ordering). Then $a \mid d$ and $b \mid d$. Let $c \in \mathbb{N} \setminus \{0\}$ be another number such that $a \mid c$ and $b \mid c$. By the assumption

on d , we have $d \leq c$. Now, by the division theorem, there exist numbers $q, r \in \mathbb{Z}$, $0 \leq r < d$ such that $c = qd + r$, i.e. $r = c - qd$. Since $a \mid d$ and $a \mid c$, we have $a \mid (c - qd)$, and similarly $b \mid (c - qd)$, i.e. $a \mid r$ and $b \mid r$. Now, $r < d$, so by the definition of d we must have that $r \leq 0$, hence $r = 0$. Thus $c = qd$, so $d \mid c$. Hence d satisfies Definition 2.

Note that there cannot be more than one number as in Definition 2, since the number in Definition 2 is a least upper bound (with respect to divisibility) and least upper bounds are unique, if they exist.

7. Let $a, m \in \mathbb{N} \setminus \{0\}$, and let $b \in \mathbb{Z}$. Show that the equation

$$ax \equiv b \pmod{m}$$

has a solution if and only if $\gcd(a, m) \mid b$.

Solution: Suppose c is a solution to

$$ax \equiv b \pmod{m}.$$

Then $m \mid b - ac$, so there exists a $q \in \mathbb{Z}$ such that $qm = b - ac$, hence $qm + ac = b$. Let $d = \gcd(a, m)$. Then $d \mid a$ and $d \mid m$, so $d \mid (qm + ac)$, i.e. $d \mid b$.

On the other hand, let $d = \gcd(a, m)$, and suppose that $d \mid b$. Then there exist $p, q \in \mathbb{Z}$ such that $ap + mq = d$ and there exists a $r \in \mathbb{Z}$ such that $rd = b$. Hence

$$apr + mqr = dr = b,$$

so $m \mid b - apr$, hence $apr \equiv b \pmod{m}$, so $x = pr$ is a solution.

8. Let $E(\mathbb{N})$ be the set of all equivalence relations on \mathbb{N} . Is $E(\mathbb{N})$ countable?

Solution: $E(\mathbb{N})$ is not countable. There is an injection $\phi : P(\mathbb{N} \setminus \{0\}) \rightarrow E(\mathbb{N})$ defined as follows: given a set $A \subseteq \mathbb{N} \setminus \{0\}$, let R_A be the equivalence relation given by

$$aR_A b \text{ iff } \begin{cases} a = b & \text{or} \\ a \in A \cup \{0\} \text{ and } b \in A \cup \{0\}. \end{cases}$$

(As partitions, this is the partition with one piece $A \cup \{0\}$ and all other pieces one-element sets.) Define $\phi(A) = R_A$. Then ϕ is injective, since ϕ has a left inverse given by sending $R \in E(\mathbb{N})$ to $\{b \in \mathbb{N} \setminus \{0\} \mid 0 \sim b\}$. Since the set $P(\mathbb{N} \setminus \{0\})$ is uncountable, we conclude that $E(\mathbb{N})$ is also uncountable.