Math 300.2 **Problem Set 9 Answers** **Fall, 2007**

1. [Exercise 2.5.4 (1).]

   (a) Yes, $41 \in [5]_{12}$ because $5 \equiv 41 \pmod{12}$. And $5 \in [41]_{12}$ because $41 \equiv 5 \pmod{12}$.

   (b) $36 \notin [5]_{12}$ because $5 \not\equiv 36 \pmod{12}$. And $5 \notin [36]_{12}$ because $36 \not\equiv 5 \pmod{12}$.

   (c) For modulus $m = 12$: For all integers a and b:

   $$b \in [a]_m \iff a \in [b]_m$$

   More generally, for *any* modulus m, the same equivalence holds.
   Proof (optional): Immediate from Lemma 2.5.3. Or prove it directly:

   $$\begin{aligned} b \in [a]_m &\iff a \equiv b \pmod{m} && \text{(definition of congruence class)} \\ &\iff b \equiv a \pmod{m} && \text{(symmetry of congruence relation)} \\ &\iff a \in [b]_m && \text{(definition of congruence class)} \end{aligned}$$

2. [Exercise 2.5.15 (4).] Let $A, B, C \in \mathbb{Z}_m$. Pick representatives a, b, c of A, B, C, respectively. Then

   $$\begin{aligned} A \cdot (B + C) &= [a] \cdot ([b] + [c]) \\ &= [a] \cdot [b + c] \\ &= [a \cdot (b + c)] \\ &= [a \cdot b + a \cdot c] \\ &= [a \cdot b] + [a \cdot c] \\ &= [a] \cdot [b] + [a] \cdot [c] = A \cdot B + A \cdot C. \end{aligned}$$

3. [Exercise 2.5.16 (d)–(f).]

   (d) *Yes,* there are such elements because, for example, $[2] \cdot [6] = [0]$ but $[2] \neq [0]$ and $[6] \neq [0]$. Another example: $[3] \cdot [4] = [0]$ but $[3] \neq [0]$ and $[4] \neq [0]$; by commutativity, other examples are $[6] \cdot [2] = [0]$ and $[4] \cdot [3]$. There are no others besides these four examples. Indeed, for $0 < a < 12$ and $0 < b < 12$, if $a \cdot b \equiv 0 \pmod{12}$ and if a is relatively prime to 12, then $b \equiv 0 \pmod{12}$, and aside from 2, 3, 4, and 6, no other integers from 1 to 11 are relatively prime to 12.

   (e) In $\mathbb{Z}_5$ there are *no* such elements. In fact, for integers $a, b \in \{0, 1, 2, 3, 4\}$, to say $[a] \cdot [b] = [0]$ but $[a] \neq [0]$ and $[b] \neq [0]$ in $\mathbb{Z}_5$ means that $5 \mid ab$ but $5 \nmid a$ and $5 \nmid b$. But this is impossible because 5 is prime.

   (f) *Generalization:* Integer m is composite if and only if there are elements $A, B \in \mathbb{Z}_m$ with $A \cdot B = [0]$ but $A \neq [0]$ and $B \neq [0]$.
   Proof: If m is prime, the same reasoning applied to the case $m = 5$ works. So suppose m is not prime. Then $m = a\,b$ for some integers a, b with $1 < a, b < m$. Then $m \mid a\,b$ but $m \nmid a$ and $m \nmid b$, so that $[a] \cdot [b] = [0]$ in $\mathbb{Z}_m$ but $[a] \neq [0]$ and $[b] \neq [0]$. □

4. [Exercise C.1.3 (b), (c), and (k).]

(b) This is *not* an equivalence relation because it is not symmetric. In fact, $1 \sim 2$ because $2 = 2 \cdot 1$ but $2 \not\sim 1$ because $1 \neq k \cdot 2$ for all nonzero integers k.

(c) This *is* an equivalence relation. In fact, it is reflexive because $|x| = |x|$ for all $x \in \mathbb{R}$. It is symmetric because if $x, y \in \mathbb{R}$ with $|x| = |y|$, then also $|y| = |x|$. and it is transitive because if $x, y, z \in \mathbb{R}$ with $|x| = |y|$ and $|y| = |z|$, then also $|x| = |z|$.

(k) This is *not* an equivalence relation because it is not reflexive: $\varnothing \in \mathcal{P}(\mathbb{R})$ yet $\varnothing \cap \varnothing = \varnothing$ so that $\varnothing \not\sim \varnothing$.

It is tempting to try to make the relation an equivalence relation by deleting the troublesome set $\varnothing$, that is, to replace $\mathcal{P}(\mathbb{R})$ by $X = \mathcal{P}(\mathbb{R}) \setminus \{\varnothing\}$. However, the restriction of the given relation just to elements of this smaller set X is still not an equivalence relation because it is *not* transitive (although it is reflexive and symmetric). In fact, there are lots of examples of nonempty subsets A, B, C of $\mathbb{R}$ for which $A \cap B \neq \varnothing$, $B \cap C \neq \varnothing$, and yet $A \cap C = \varnothing$; for example, take $A = \{1\}$, $B = \{1, 2\}$, and $C = \{2\}$.

5. [Prop. C.1.8.] Let A and B be equivalence classes under $\sim$. Choose representatives a and b of A and B, respectively, so that $A = [a]$ and $B = [b]$.

   Assume $A \cap B \neq \varnothing$. Then there exists some $z \in A \cap B$. By part (3) of the lemma, $[z] = [a]$ and $[z] = [b]$, that is, $[z] = A$ and $[z] = B$. Then $A = B$. $\square$

6. [Exercise C.1.9 (2) (a).]

   - *reflexive:* If $(m, n) \in X$, then $(m, n) \sim (m, n)$ because $m\,n = n\,m$.
   - *symmetric:* Let $(m, n), (i, j) \in X$. If $(m, n) \sim (i, j)$, then $m\,j = n\,i$ so that $i\,n = j\,m$ which means $(i, j) \sim (m, n)$.
   - *transitive:* Let $(m, n), (i, j), p, q \in X$ with $(m, n) \sim (i, j)$ and $(i, j) \sim (p, q)$. Then

     $$m\,j = n\,i \text{ and } i\,q = j\,p.$$

     Multiply the first equality by q and in the result use the second equality to substitute for $i\,q$:

     $$m\,j\,q = n\,i\,q = n\,j\,p.$$

     Now $j \neq 0$, so divide by j to obtain

     $$m\,q = n\,p.$$

     This means that $(m, n) \sim (p, q)$.

   For integers m, n with $n \neq 0$, the equivalence class $[(m, n)]$ of course is given by

   $$[(m, n)] = \{\, (i, j) \in \mathbb{Z} \times \mathbb{Z}^* : m\,j = n\,i \,\}.$$

   It is more illuminating, however, to think of this as:

   $$[(m, n)] = \left\{ (i, j) \in \mathbb{Z} \times \mathbb{Z}^* : \frac{m}{n} = \frac{i}{j} \right\}$$

7. [Exercise C.2.6 (b).] First, the collection $\mathcal{A}$ is a partition of X: Obviously no member of $\mathcal{A}$ is empty. If $x = 0$ or $x = 1$, then $x \in \{0, 1\} \in \mathcal{A}$, whereas if $x \in [0, 1]$ and if $x \neq 0, 1$, then $x \in \{x\} \in \mathcal{A}$; thus each $x \in X$ belongs to some member of $\mathcal{A}$. Finally, $\{0, 1\} \cap \{t\} = \varnothing$ if $0 < t < 1$, and $\{t\} \cap \{s\} = \varnothing$ if $0 < t, s < 1$ with $t \neq s$; thus $\mathcal{A}$ is pairwise disjoint.

   The definition of the equivalence relation $\sim_{\mathcal{A}}$ is that by $x \sim_{\mathcal{A}} y$ if and only if there exists some $A \in \mathcal{A}$ with $x, y \in A$. For the given partition $\mathcal{A}$, this means:

   $$x \sim_{\mathcal{A}} y \iff x, y \in \{0, 1\} \text{ or } x, y \in \{t\} \text{ for some } t \text{ with } 0 < t < 1,$$

   in other words,

   $$x \sim_{\mathcal{A}} y \iff x = y = 0 \text{ or } x = y = 1 \text{ or } (x = 0 \ \& \ y = 1) \text{ or } (x = 1 \ \& \ y = 0) \text{ or } 0 < x = y < 1.$$

   This may be simplified to:

   $$x \sim_{\mathcal{A}} y \iff (x = 0 \ \& \ y = 1) \text{ or } (x = 1 \ \& \ y = 0) \text{ or } (x = y).$$

   You could express this in words: Two numbers in $[0, 1]$ are equivalent for $\sim_{\mathcal{A}}$ when either they are identical or else one of them is 0 and the other is 1. (Put most simply, this equivalence relation "identifies" 0 with 1.)

8. [Exercise 1, *Reals*.]

   (a) Let $x \in \mathbb{R}$ and assume $0 < x$. Since $x = 0 + x = 0 - (-x)$, then $0 < 0 - (-x)$. This means $-x < 0$.

   (b) Let $x, y \in \mathbb{R}$ and assume $x < y$. Then $0 < y - x$. Now $(-x) - (-y) = y - x$, so $0 < (-x) - (-y)$. This mean $-y < -x$.

   (c) Exactly one of the alternatives cases $0 < 1$, $0 = 1$, and $1 < 0$ holds. Now $0 \neq 1$. Just suppose $1 < 0$. From (b), $-0 < -1$, that is, $0 < -1$. From the third property of $<$ above, $0 < (-1)(-1)$. But $(-1)(-1) = 1$, so that $0 < 1$, which is impossible when also $1 < 0$.

9. [Prop. 2 proof details, *Reals*.]

   (a) [Why is $n \leq c < n + 1$?] By definition, $k_1 > c$ and, for each $k \in \mathbb{N}$, $k < k_1 \implies k \leq c$. Now $k_1 \neq 0$ because $c > 0$. Hence $k_1 \geq 1$. Thus $n = k_1 - 1 \in \mathbb{N}$. Since $n < k_1$, then $n \leq c$. And of course $n + 1 = k_1 > c$.

   (b) [Finish proof of Case (ii).] If $m = -c$, then $-m = c < -m + 1$. Suppose now $m \neq -c$, so that $m < -c < m + 1$. Then $-m - 1 < c < m$, and so $-m - 1 \leq c < (-m - 1) + 1$.

   (c) [Uniqueness.] Suppose m and n are both integers with $m \leq c < m + 1$ and $n \leq c < n+1$. Just suppose $m \neq n$, say $m < n$. Then $m+1 \leq n$, and so $m+1 \leq n < c < n+1$. But also $m \leq c < m+1$, so that $m \leq c < m+1 \leq n < c < n+1$. Thus $c < m + 1$ and $c > m + 1$, which is impossible.

10. [Re Theorem 3 proof, *Reals*.]

(a) We are given that $a < b$. So if $0 \leq a$ is not the case, we are left with one of the following cases:

Case (i): $a < b < 0$. In this case $0 < -b < -a$. From the already-proved case, there exists $q \in \mathbb{Q}$ with $-b < q < -a$. Then $-q \in \mathbb{Q}$ and $a < -q < b$.

Case(ii): $a < 0 < b$. From the already-proved case, there exists $q \in \mathbb{Q}$ with $0 < q < b$. Then $a < q < b$ also.

(b) By Proposition 2, there exists an integer k with $k \leq nc < k + 1$. Now $nc > 0$ because $n > 0$ and $c > 0$. Thus $k \geq 0$. Let $m = k + 1$. Then $m \in \mathbb{N}$ and $m - 1 = k \leq nc < k + 1 = m$.