Proofs in Contemporary Math  
W. J. Martin  
April 4, 2009  

MA196X Problem Set 3

**Instructions:** Please first read the rules on the presentation of assignments in the course. Then complete as many of these as you can by Friday, April 10th. After that, I will still accept problems until the sample solutions have been distributed.

**Note:** Always identify each problem by its problem number and re-state the problem precisely before giving its solution.

13. (a) Prove: For all sets $A$ and $B$ and all relations $r, s$ from $A$ to $B$, we have $\text{Dom}(r \cup s) = \text{Dom}(r) \cup \text{Dom}(s)$. (Then show that, without further proof, it follows that $\text{Im}(r \cup s) = \text{Im}(r) \cup \text{Im}(s)$.)

(b) Show that the following proposition is false: For all sets $A$ and $B$ and all relations $r, s$ from $A$ to $B$, we have $\text{Dom}(r \cap s) = \text{Dom}(r) \cap \text{Dom}(s)$.

14. Prove: If $r$ is a relation on set $A$ with $\text{Dom}(r) = A$ and $r$ is both symmetric and transitive, then $r$ is reflexive.

15. Prove: If $A$ is any set and $r$ is a relation on $A$, then $r$ is both symmetric and antisymmetric if and only if $r \subseteq \text{id}_A := \{(a, a) : a \in A\}$.

16. Suppose $A$ is a non-empty set and consider the relation $r$ defined on $\mathcal{P}(A)$ by

$$ArB \iff A \cap B = \emptyset.$$  

In parts (a)-(e), decide whether the given statement is TRUE or FALSE. If it is true, provide a proof; if it is false, provide a simple counterexample.

(a) $r$ is reflexive

(b) $r$ is irreflexive

(c) $r$ is symmetric

(d) $r$ is antisymmetric

(e) $r$ is transitive

17. Let $A$, $B$ and $C$ be sets. Let $r$ be a relation from $A$ to $B$ and let $s$ be a relation from $B$ to $C$. For these objects, define

$$s \circ r = \{(a, c) \in A \times C \mid \exists b \in B \ (arb \land bsc)\}.$$  

Prove: For any $A$, $B$, $C$ and any $r \subseteq A \times B$ and $s \subseteq B \times C$, $\text{Dom}(s \circ r) \subseteq \text{Dom}(r)$ and $\text{Im}(s \circ r) \subseteq \text{Im}(s)$.  

1
18. With notation as in the previous problem, prove: if \( B = C \) and \( s = \text{id}_B \), then \( s \circ r = r \).

19. With notation as in Problem 17, prove: if \( \text{Im}(r) = \text{Dom}(s) \), then \( \text{Dom}(s \circ r) = \text{Dom}(r) \) and \( \text{Im}(s \circ r) = \text{Im}(s) \). [NOTE: If you have previously solved Problem 17, then you may use its result in your solution.]

20. Let \( A \) be a non-empty set and let \( r \) and \( s \) be relations on \( A \). For each of the following propositions, decide whether the statement is true or false. If it is true, prove it; if the statement is false, give a simple counterexample.

(a) If both \( r \) and \( s \) are reflexive, then \( s \circ r \) is reflexive.
(b) If both \( r \) and \( s \) are irreflexive, then \( s \circ r \) is irreflexive.
(c) If both \( r \) and \( s \) are symmetric, then \( s \circ r \) is symmetric.
(d) If both \( r \) and \( s \) are antisymmetric, then \( s \circ r \) is antisymmetric.
(e) If both \( r \) and \( s \) are transitive, then \( s \circ r \) is transitive.

21. In number theory, we make extensive use of the “exactly divides” relation. The relation \( \parallel \subseteq \mathbb{Z} \times \mathbb{Z} \) is defined as follows: for a prime \( p \), and integer \( n \) and a positive integer \( k \),
\[
p^k | n \leftrightarrow [(p^k | n) \land (\forall \ell \in \mathbb{Z}) (\ell > k \rightarrow p^\ell \not| n)];
\]
in all other cases, \( m | n \) is false.

(a) Find \( \text{Dom}(\parallel) \). Explain briefly.
(b) Find \( \text{Im}(\parallel) \). Explain briefly.
(c) Show that, for any prime \( p \) and any \( k \geq 1 \), the set \( \{ n \in \mathbb{Z} : p^k | n \} \) is infinite.
(d) For \( n \in \mathbb{Z} \), arbitrary but fixed, what can you conclude about the size of the set \( \{ m \in \mathbb{Z} : m | n \} \)? Justify.

22. Let \( m \) and \( n \) be positive integers. Let \( r \) be the relation “congruence modulo \( m \)” on \( \mathbb{Z} \) and let \( s \) be the relation “congruence modulo \( n \)” on \( \mathbb{Z} \) (see p44 for the definition). Prove: if \( n | m \), then \( r \subseteq s \).

23. Prove: For any positive integer \( n \) and for all integers \( a, b, c, d \), if \( a \equiv b \mod n \) and \( c \equiv d \mod n \), then
\[
a + c \equiv b + d \mod n \quad \text{and} \quad ac \equiv bd \mod n.
\]

24. Let \((A, \preceq)\) be a finite poset (i.e., \( A \) is a finite set and \( \preceq \) is a partial order relation on \( A \)). Prove that there exists a linear extension for \( \preceq \): there exists a total order relation \( \preceq_* \), extending \( \preceq \) (i.e., \( \preceq \subseteq \preceq_* \subseteq A \times A \)). (See p61 for the definition.)