PMAT 315 Winter 2007

ASSIGNMENT 1

due Friday February 2.

1. (a) Prove that, for all $a, b, c, d \in \mathbb{Z}^+$,

$$\Big(d|\gcd(a,b) \text{ and } d|c\Big) \text{ if and only if } \Big(d|a \text{ and } d|\gcd(b,c)\Big).$$

You may use the fact (which follows from Theorem 0.2 on page 5) that for all $a, b, d \in \mathbb{Z}^+$, if $d|a$ and $d|b$ then $d|\gcd(a,b)$.

(b) Use part (a) to prove that $\gcd(\gcd(a,b),c) = \gcd(a, \gcd(b,c))$ for all $a, b, c \in \mathbb{Z}^+$.

(c) Define the binary operation $\circ$ on $\mathbb{Z}^+$ by: for any $a, b \in \mathbb{Z}^+$, $a \circ b = \gcd(a,b)$. Is $\circ$ associative? Explain.

(d) Is $(\mathbb{Z}^+, \circ)$ a group? Explain.

2. (a) Let S be the set of all even integers. For any $a, b \in \mathbb{Z}$, define aRb if and only if $a + b \in S$. Prove that R is an equivalence relation on $\mathbb{Z}$. [This is almost the same as exercise 50 on page 26.]

(b) Suppose we change the set S in part (a) to be some other subset of $\mathbb{Z}$. Prove that if S does not contain every even integer, then R is not an equivalence relation on $\mathbb{Z}$.

(c) Again suppose we change the set S in part (a) to be some other subset of $\mathbb{Z}$. Prove that if S contains every even integer and also at least one odd integer, but $S \neq \mathbb{Z}$, then R is not an equivalence relation on $\mathbb{Z}$.

3. For any $a, b \in \mathbb{Z}$, let $a \circ b = a + b - 2$. Prove that $(\mathbb{Z}, \circ)$ is a group.

4. Page 54 #19. Do it for positive integers n only. Use induction on n.

5. Page 54 #31. [$\exists$ a big hint in the back of the text!]