Math 371 Problem Set #3 Due week of Feb. 4, 2008, in lab.

Read Herstein, Chapter 3, sections 1-2.

1. From Herstein, do these problems:

a) Chapter 1, Section 1.3, page 24: #10 [i.e. prove both forms of induction using well ordering], #14 [Hint: If p doesn't divide a, show that the elements $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ in $\mathbb{Z}/p$ form a permutation of the elements $1, 2, \ldots, p-1$ and so have the same product], #15 [Hint: First do this for the case $a = 1$ and $b = 0$, then for $a = 0$ and $b = 1$, and then combine those to get the general case].

b) Chapter 3, Section 3.2, page 130: #2 [and also give an example to show that this is not always the same as $a^2 + 2ab + b^2$].

2. a) Applying the Euclidean algorithm (cf. Hersetin, p.24, #6-7) to the integers 324 and 45, and then working backwards, solve the Diophantine equation $324x + 45y = 9$ (i.e. find a solution in integers).

b) Do the same for $369x + 324y = 9$.

c) What about the equation $369x + 324y = 1$?

d) What about the equation $121x + 101y = 1$?

e) Use (d) to find a multiplicative inverse for 101 in $\mathbb{Z}/121\mathbb{Z}$. Can you find a multiplicative inverse for 324 in $\mathbb{Z}/369\mathbb{Z}$, either by using (c) or some other method? Explain.

3. Let R be a ring. Suppose that the elements of $R - \{0\}$ form an abelian group under multiplication. Show that R is a field.

4. a) Show that every subring of $\mathbb{R}$ contains $\mathbb{Z}$ as a subring.

b) Find a ring R that does not contain (a copy of) $\mathbb{Z}$ as a subring.

5. Which of the following are rings? For that that are: are they commutative? integral domains? fields? Explain.

i) $M_3(\mathbb{Z}/2)$

ii) $GL_3(\mathbb{Z}/2)$

iii) $\mathbb{Z}/27$

iv) $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$

v) $\{a + b\sqrt[3]{3} \mid a, b \in \mathbb{Z}\}$

vi) $\mathbb{Z} \times \mathbb{Z}$ under the addition law $(a, b) + (c, d) = (a + c, b + d)$ and multiplication law $(a, b) \cdot (c, d) = (ac, bd)$

vii) $\mathbb{R} \times \mathbb{R}$ under the addition law $(a, b) + (c, d) = (a + c, b + d)$ and multiplication law $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.