Math 371 Problem Set #6 Due week of Feb. 25, 2008, in lab.

Read Herstein, Chapter 3, sections 10-11.

1. From Herstein, Chapter 3, do these problems:

a) Section 3.7, page 149: #8.

b) Section 3.9, page 158-159: #3, 4, 7. [Hint for #4(c): Find a solution to $X^2 + X + 4$ in the field of part (a).]

c) Section 3.10, page 161: #2, 3. [Hint for #3: Let $y = x+1$ and write $x(1+y+\cdots+y^{p-1}) = (y-1)(1+y+\cdots+y^{p-1}) = y^p - 1 = (x+1)^p - 1$. Then use the binomial theorem to find an expression for $1 + y + \cdots + y^{p-1}$ and apply Eisenstein to that polynomial.]

d) Section 3.11, page 166: #11.

2. Let K be a field, $\alpha \in K$, and $f(x) \in K[x]$ a non-zero polynomial.

a) Show that there exists $q(x) \in K[x]$ satisfying $f(x) = (x - \alpha)q(x) + f(\alpha)$. [Hint: Division algorithm.]

b) Deduce that α is a root of $f(x)$ if and only if $x - \alpha$ divides $f(x)$ in $K[x]$.

c) Show that if $\alpha_1, \ldots, \alpha_m \in K$ are distinct roots of $f(x)$, then $f(x)$ is divisible by $(x - \alpha_1)\cdots(x - \alpha_m)$. [Hint: Induction and (b).]

d) Conclude that if f has m distinct roots, then the degree of f is at least m.

3. Let p be a prime number other than 2.

a) Let $a, b \in \mathbb{Z}/p$. Show that $a^2 = b^2$ if and only if $a = \pm b$.

b) Deduce that $\mathbb{Z}/p$ contains exactly $(p-1)/2$ non-zero squares (i.e. elements of the form c^2 for some $c \in \mathbb{Z}/p$).

c) Show that if $a \in \mathbb{Z}/p$ is non-zero, then $a^{p-1} = 1$ in $\mathbb{Z}/p$. [Hint: See Herstein, page 24, #14 (done on Problem Set #3).]

d) Deduce that if $a \in \mathbb{Z}/p$ is non-zero then $a^{(p-1)/2} = \pm 1$, and that if $a \in \mathbb{Z}/p$ is a non-zero square then a is a root of the polynomial $f(x) = x^{(p-1)/2} - 1$.

4. Let p be a prime number other than 2.

a) Suppose that $a \in \mathbb{Z}/p$ is non-zero. Show that a is a square in $\mathbb{Z}/p$ if and only if $a^{(p-1)/2} = 1$ in $\mathbb{Z}/p$, and a is not a square if and only if $a^{(p-1)/2} = -1$ in $\mathbb{Z}/p$. [Hint: Problem 2(d) and problem 3.]

b) Use part (a) to show that -1 is a square modulo p if and only if $p \equiv 1 \pmod 4$.

c) For each of $p = 5, 7, 11, 13$, either find a $\sqrt{-1}$ in $\mathbb{Z}/p$ or show that none exists.