Math 503 Problem Set #5 Due the week of Feb. 12, 2007, in lab.

Read Artin, Chapter 11, sections 1-3, 5.

Part A:
From Artin, do these problems (given at the end of Chapter 11):
Section 11.1: 1, 15; 11.2: 8 [Hint: Euclidean algorithm]; 11.3: 4, 9; 11.5: 1, 3.

Part B:
1. Let $p > 2$ be a prime number and let $a \in \mathbb{Z}$ be relatively prime to p.
a) Show that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.
b) Show that a is congruent to a square modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. [Hint: What is the structure of the group $\mathbb{F}_p^\times$?]

2. If $R \subset S$ are commutative rings and $I \subset R$ is an ideal of R, let $IS \subset S$ be the set of all finite S-linear combinations of elements of I. Call IS the *extension* of I to S. If $J \subset S$ is an ideal of S, call $J \cap R \subset R$ the *contraction* of J to R.
a) Are extensions and contractions always ideals? Are extension and contraction inverse operations?
b) For which prime ideals of $\mathbb{Z}$ is the extension to $\mathbb{Z}[i]$ also prime?
c) Show that taking contraction induces a surjection from the prime ideals of $\mathbb{Z}[i]$ to the prime ideals of $\mathbb{Z}$. Is it injective?
d) Do your assertions in part (c) hold for an arbitrary extension of integral domains $R \subset S$?

3. Let $\zeta = (-1 + \sqrt{-3})/2 \in \mathbb{C}$ and let $R = \mathbb{Z}[\zeta]$.
a) Show that ζ is a primitive cube root of unity. Find all other primitive cube roots of unity in $\mathbb{C}$. Also find the minimal polynomial of ζ over $\mathbb{Q}$.
b) Show that R is a subring of $\mathbb{Q}[\sqrt{-3}]$, and determine which elements $a + b\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ (for $a, b \in \mathbb{Q}$) lie in R.
c) Show that R is isomorphic to $\mathbb{Z}[x]/(x^2 + x + 1)$.
d) Show that R is a Euclidean domain. [Hint: Define a norm, and look at a picture of R in $\mathbb{C}$.] Is R a PID? a UFD?

Part C:
From Artin, do these problems (at the end of Chapters 10 and 11):
Section 10.7: 13 (and explicitly describe the case $R = \mathbb{Z}$ and $P = (2)$); 10.8: 8 (and explicitly describe the case $R = \mathbb{C}[x]/(x^3)$); 11.5: 8 (and in part (a), show this is also equivalent to there being an element of order 3 in $\mathbb{F}_p^\times$).

Also do the following problem:
For each positive integer n, let $U_n = (\mathbb{Z}/n)^\times$, the group of units modulo n. Find generators of U_5 and U_{25}, and determine whether there exist generators of U_{27} and U_{21}. Conjectures? Proofs?