Math 503 Problem Set #6 Due the week of Feb. 19, 2007, in lab.

Read Artin, Chapter 11, sections 4-11.

Part A:
From Artin, do these problems (given at the end of Chapter 11):
Section 11.4: 1(a,c,e); 11.5: 2; 11.6: 1 (verify explicitly); 11.8: 1; Miscellaneous problems: 1-3. [Hint: Do #3 first, taking $4P-1$, where P is a suitable product of primes. For #1, consider the Gaussian factorization of $4Q^2+1$, where Q is a suitable product of primes.]

Part B:
1. If $I, J \subset R$ are ideals in a commutative ring, define the *ideal quotient* $(I : J) \subset R$ to be $\{a \in R \,|\, aJ \subset I\}$. Show that this is an ideal. If $R = \mathbb{Z}$, prove that $((m) : (n)) = (m/\gcd(m,n))$.

2. Show there exist infinitely many primes in $\mathbb{Z}[i]$ that lie on an axis, and infinitely many primes in $\mathbb{Z}[i]$ that do not lie on an axis.

3. a) Which of the following rings are integrally closed?
$\mathbb{R}[x]$, $\mathbb{R}[x,y]/(y^2-x)$, $\mathbb{R}[x,y]/(y^2-x^3)$, $\mathbb{R}[x,y]/(y^2-x^2-x^3)$.
[Hint: See part (d) of the problem in Part C of PS#3.]

b) For each ring in (a), draw the corresponding variety on which it is the ring of functions. Any conjectures about the relationship between the geometry of the curve and whether the ring is integrally closed?

4. a) If ℓ is a prime, for which positive integers n is there a primitive n^{th} root of unity in $\mathbb{F}_\ell$? [Hint: What is the structure of the group $\mathbb{F}_\ell^\times$?]

b) Given a prime number p, for which primes ℓ does the cyclotomic polynomial $\Phi_p(x)$ factor as a product of distinct monic linear factors? [Hint: Use part (a).]

Part C:
From Artin, do these problems (at the end of Chapter 11):
Section 11.7: 2, 9 (and deduce the ring is not a PID); Miscellaneous: 4.

Also do the following problem:

a) Show that $R = \mathbb{Z}[\sqrt{2}]$ is a Euclidean domain. [Hint: Consider the lattice in Chapter 11 Fig. 11.3, and for $\alpha \in R$ let $\sigma(\alpha)$ be the square of the distance from the origin to the lattice point corresponding to α.] Is R a PID? a UFD?

b) Show that a prime number $p > 0$ factors non-trivially in R if and only if $\pm p$ is of the form $a^2 - 2b^2$ for some $a, b \in \mathbb{Z}$. [Hint: For $\alpha = a + b\sqrt{2} \in R$ (with $a, b \in \mathbb{Z}$), let $\overline{\alpha} = a - b\sqrt{2}$, and consider the norm $N(\alpha) = \alpha\overline{\alpha}$.]

c) Show that a prime number $p > 0$ remains prime in R if and only if there is no square root of 2 in $\mathbb{F}_p$. [Hint: Mimic the proof for $\mathbb{Z}[i]$.]

d) For $p = 3, 5, 7, 17$, determine whether p remains prime in R, and whether there exist integers a, b such that $a^2 - 2b^2 = \pm p$.