Math 503 Problem Set #7 Due the week of Feb. 26, 2018, in lab.

Read Artin, Chapter 12, sections 3,4; and Chapter 13, sections 1,2,4 (optional: section 3).

1. a) From Artin, Chapter 12, do these problems (pages 378-382): 3.1(a), 3.2, 4.2, 4.3.
b) From Artin, Chapter 13, do these problems (pages 408-411): 1.1 (verify this explicitly), 1.2.

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 (see PS4, problem 5).
a) Are extensions 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?

4. 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 $((m) : (n)) = (m/\gcd(m, n))$.

5. a) Show that there are infinitely many prime numbers $p > 1$ that are congruent to -1 mod 4. [Hint: Mimic the proof that there are infinitely many primes, but take $4P - 1$, where P is a suitable product of prime numbers.]
b) Show that there are infinitely many prime numbers $p > 1$ that are congruent to 1 mod 4. [Hint: Consider the Gaussian factorization of $4Q^2 + 1$, where Q is a suitable product of prime numbers.]
c) 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. [Hint: Use parts (a) and (b).]