Math 113 Homework 9. Due 11/10

Reading corresponding to lectures:
Tuesday 11/3 DF 7.5 Thursday 11/5 DF 7.6, beginning of 8.1 if time.
Tuesday 11/6 DF 8.1, 8.2
Note: On Tuesday, 11/17, you have a 30-minute test.

Problems to hand in:

1. Recall the quadratic integer ring $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$. Show that $\mathbb{Z}[i]$ is an integral domain, and describe its field of fractions. You should use the fact that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, and that you know how to divide complex numbers.
   Optional: can you generalize this to $\mathbb{Z}[\sqrt{-D}]$?

2. Let F be the field of fractions of $2\mathbb{Z}$. Prove that F is isomorphic (as a ring) to $\mathbb{Q}$, by showing that $\phi : F \to \mathbb{Q}$ defined by $\phi(\frac{2a}{2b}) = \frac{a}{b}$ is a bijective ring homomorphism.

3. Do problem 4 from DF section 7.5 (possible hint: show that any subring of $\mathbb{R}$ contains $\mathbb{Z}$, then apply corollary 16 from section 7.5)

4. Do the following problems from DF section 7.6: 3, 4, 7
   Note: problem 5 in this section was discussed in class, you might find it helpful to review as a way of comparing the C.R.T. for $\mathbb{Z}$ and for general rings.

5. Use the Chinese remainder theorem for $\mathbb{Z}$ to find the smallest positive integer x that satisfies the following system of equations
   $x \equiv 4 \pmod 5$
   $x \equiv 6 \pmod 8$
   $x \equiv 8 \pmod 9$

6. Let $R = \mathbb{R}[x]$. Let A be the ideal generated by $(x + 3)$ and B be the ideal generated by $(x + 5)$.
   (a) Show that A and B are "relatively prime" (or "comaximal" in the language of DF)
   (b) The Chinese remainder theorem says that there exists a polynomial $p(x)$ satisfying $p(x) + A = x^2 + A$, (i.e. $p(x) \equiv x^2 \mod A$) and $p(x) + B = 3x + B$. Find such a polynomial $p(x)$. (You can find one that is degree 1).
   (c) Suppose that $p(x)$ and $q(x)$ were two different solutions to the above system of equations. What does the Chinese remainder theorem say about the relationship between $p(x)$ and $q(x)$?
   (d) Why did I say that there was a solution $p(x)$ of degree 1?

7. Let $p_1, p_2, ...p_k$ be distinct primes in $\mathbb{Z}$, and let n be their product, $n = p_1p_2...p_k$.
   (a) Use the Chinese remainder theorem on the ring $R = \mathbb{Z}/n\mathbb{Z}$ to show that
   $$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times ... \times \mathbb{Z}/p_k\mathbb{Z}$$
   (b) What are the units (elements with multiplicative inverses) in the ring $\mathbb{Z}/p_1\mathbb{Z} \times ... \times \mathbb{Z}/p_k\mathbb{Z}$?
   (c) The *Euler ϕ function*, defined on the natural numbers, is given by $\phi(n) =$ number of units in $\mathbb{Z}/n\mathbb{Z}$. If $n = p_1, p_2, ...p_k$ is a product of distinct primes, use your work above to compute $\phi(n)$.

   Challenge, not to hand in: How does this problem generalize if we replace the primes with *powers* of primes, i.e. $n_i = p_i^{\alpha_i}$