Introduction to Algebra, MATH 5127

Homework 11, Sections IV.20 and IV.21

Due Friday April 26, 2013 at 2:30

20.5. Use the Little Theorem of Fermat to find the remainder when 37^{49} is divided by 7. Explain your computations.

20.9. Compute $\varphi(pq)$ where p and q are distinct primes. Is $\varphi(pq) = \varphi(p^2)$ when $q = p$?

20.27. Show that 1 and $p - 1$ are the only elements of the field $\mathbb{Z}_p$ (p prime) that are their own multiplicative inverse. HINT: Explain why a being its own inverse is equivalent to a being a solution to $x^2 - 1 = 0$. Find all solutions to $x^2 - 1 = 0$ in $\mathbb{Z}_p$.

21.1. Let $D = \{n + mi \mid n, m \in \mathbb{Z}\}$. This is an integral subdomain of $\mathbb{C}$ called the *Gaussian integers*. With the notation of page 191, describe the sets $D \times D$ and S. What are the equivalence classes of the set S? What are the elements of $i[D]$? HINT: To find the quotient of two complex numbers (the elements of $i[D]$), you will need to use complex conjugates (see equation (7) on page 15).

21.11. Prove that the distributive law holds in F, as claimed in "Step 3" of page 193:

$$[(a, b)] \cdot ([c, d] + [r, s]) = [(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(r, s)].$$

21.12. Let R be a commutative ring with at least two elements. Let T be a nonempty subset of R that is closed under multiplication and which contains neither 0 nor divisors of 0. The argument of this section can be followed, but by replacing $D \times D$ with $R \times T$, to produce a *partial ring of quotients* $Q(R, T)$.

(a) Prove that $Q(R, T)$ has unity even if R does not.

(b) For $a \in T$, prove that $[(aa, a)] \in Q(R, T)$ is a unit.

21.13. (Bonus). Use Exercise 21.12 to prove that any commutative ring containing an element $a \neq 0$, where a is not a divisor of zero, can be enlarged to a commutative ring with unity. HINT: Let $T = \{a^n \mid n \in \mathbb{N}\}$. Show that T satisfies the hypotheses of Exercise 21.12. Show that the resulting ring is commutative.