HOMEWORK 5, DUE THURSDAY FEBRUARY 15TH

1. Chapter 4, §5: 10, 13 (*Hint: you might find it easier not to use the hint*), 14, 19.
2. Chapter 4, §6. 1, 2, 3, 6-14.
3. Chapter 5, §1. 3, 4.

Challenge Problems: (Just for fun)

4. Chapter 4, §5: 23, 24, 25.
5. We are going to give another proof that if p is a prime congruent to 1 modulo 4 then p is the sum of two squares, $p = a^2 + b^2$, where a and b are natural numbers.

We first suppose that p is any prime.
(a) Which elements of $\mathbb{F}_p$ are their own inverses?
(b) Show that

$$(p-1)!$$

is congruent to -1 modulo p.
Now suppose that p is congruent to 1 modulo 4.
(c) Show that the square of

$$\prod_{a=1}^{(p-1)/2} a$$

is -1 modulo p.
(d) Show that there is a natural number m such that m^2+1 is divisible by p.
(e) Conclude that p is not a prime element in the Gaussian integers.
(f) Show that there are natural numbers a and b such that

$$p = a^2 + b^2.$$