HOMEWORK 3, DUE THURSDAY FEBRUARY 1ST

1. Chapter 4, Section 4: 1, 2, 7, 8.
2. Let R be a ring and let I be an ideal of R, not equal to the whole of R. Suppose that every element not in I is a unit. Prove that I is the unique maximal ideal in R.
3. Let $\phi\colon R \longrightarrow S$ be a ring homomorphism and suppose that J is a prime ideal of S.
(i) Prove that $I = \phi^{-1}(J)$ is a prime ideal of R.
(ii) Give an example of an ideal J that is maximal such that I is not maximal.
4. Prove that every prime element of an integral domain is irreducible.
Let R be a commutative ring. Our aim is to prove a very strong form of the Chinese Remainder Theorem. First we need some definitions. Let I and J be two ideals. We say that I and J are **coprime** if $I + J = R$.
5. (a) Show that I and J are coprime if and only if there is an $i \in I$ and a $j \in J$ such that $i + j = 1$.
(b) Show that if I and J are coprime then $IJ = I \cap J$.
Suppose that $I_1, I_2, \dots, I_k$ are ideals of R. We say these ideals are **pairwise coprime**, if for all $i \neq j$, I_i and I_j are coprime.
6. If $I_1, I_2, \dots, I_k$ are pairwise coprime, show that the product I of the ideals $I_1, I_2, \dots, I_k$ is equal to the intersection, that is

$$\prod_{i=1}^{k} I_i = \bigcap_{i=1}^{k} I_i.$$

(*Hint. Proceed by induction on* k).
Let R_i denote the quotient R/I_i. Define a map,

$$\phi\colon R \longrightarrow \bigoplus_{i=1}^{k} R_i,$$

by $\phi(a) = (a + I_1, a + I_2, \dots, a + I_k)$
7. (a) Show that ϕ is a ring homomorphism.
(b) See below.
(c) Show that ϕ is injective if and only if I, the intersection of the ideals $I_1, I_2, \dots, I_k$, is equal to the zero ideal.
8. Deduce the Chinese Remainder Theorem, which states that if $I_1, I_2, \dots, I_k$ are pairwise coprime and the product I is the zero ideal, then R is

isomorphic to $\oplus_{i=1}^{k} R_i$. Show how to deduce the other versions of the Chinese Remainder Theorem, which are stated as exercises in the book.

Challenge Problems: (Just for fun)

7 (b) Show that ϕ is surjective if and only if the ideals $I_1, I_2, \dots, I_k$ are pairwise coprime.
9. (i) Let K be field and let R be the ring of all formal sums $a + b\epsilon$, where a and $b \in K$. Define an addition and a multiplication on R by the rules

$$(a + b\epsilon) + (c + d\epsilon) = (a + b) + (c + d)\epsilon \qquad \text{and} \qquad ac + (ad + bc)\epsilon,$$

so that, in particular, $\epsilon^2 = 0$.
Show that with this rule of addition and multiplication, R becomes a ring.
(ii) Show that R is isomorphic to

$$\frac{K[x]}{\langle x^2 \rangle}.$$

10. Let $p \in \mathbb{N}$ be a prime.
(i) Show that if we may find natural numbers a and b such that $p = a^2 + b^2$ then p is not congruent to 3 modulo 4 (*Hint: consider the possibilities for* a^2 *modulo* 4).
(ii) Show that 2 is a sum of two squares.
(iii) Suppose that p is congruent to 1 modulo 4. Consider the set

$$S = \{\, (x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p \,\}.$$

Show that S has two involutions, the easy one

$$(x, y, z) \longrightarrow (x, z, y)$$

and the less obvious one

$$(x, y, z) \longrightarrow \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } 2y < x. \end{cases}$$

(iv) Show that the less obvious one has exactly one fixed point. Conclude that we may find a and b such that $p = a^2 + b^2$.
11. Let $p \in \mathbb{N}$ be a prime. Show that p is a prime element of the Gaussian integers if and only if p is congruent to 3 modulo 4.