MODEL ANSWERS TO THE THIRD HOMEWORK

2. Chapter 4, §4: 1. Note that if 3 does not divide a, then either a is congruent to 1 or 2 modulo 3. Either way a^2 is congruent to $1 = 1^2 = 2^2$ modulo three. In this case $a^2 + b^2$ is congruent to either $1 = 1 + 0$ or $2 = 1 + 1$, modulo three. Thus 3 does not divide $a^2 + b^2$.
2. It is proved in example 2 that M is maximal so that R/M is a field and so it suffices to prove that R/M has cardinality 9. There are two ways, essentially equivalent, ways to proceed. The first is to observe that $a+bi$ and $c+di$ generate the same left coset if and only if $(a-c)+(b-d)i \in I$, that is 3 divides $a-c$ and 3 divides $b-d$. In turn, this is equivalent to saying that a and c (respectively b and d) have the same residue modulo 3. As there are 3 residues modulo three, namely 0, 1 and 2, there are $9 = 3 \times 3$ left cosets, and R/M has cardinality 9. The second way to proceed is to define a map

$$\phi \colon \mathbb{Z}[i] \longrightarrow \mathbb{Z} \oplus \mathbb{Z},$$

by sending $a + bi$ to (a, b). It is easy to check that this map is a group homomorphism (and just as easy to see that it is *not* a ring homomorphism). Under this correspondence, I corresponds to $3\mathbb{Z} \oplus 3\mathbb{Z}$ and so the cardinality of R/M is equal to the cardinality of

$$\frac{\mathbb{Z} \oplus \mathbb{Z}}{3\mathbb{Z} \oplus 3\mathbb{Z}} \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3,$$

which, as before, is $9 = 3 \times 3$.
7. First note that, as $\sqrt{2}$ is irrational, then

$$a + b\sqrt{2} = c + d\sqrt{2},$$

if and only if $a = c$ and $b = d$. Indeed if $b = d$, then this is clear. Otherwise, we can solve for $\sqrt{2}$ to obtain

$$\sqrt{2} = \frac{a-c}{d-b} \in \mathbb{Q},$$

a contradiction. Thus the fact that R/M has 25 elements follows, as in 2.
It remains to prove that M is maximal. Given two integers a and b, consider $a^2 - 2b^2$. As before, the key point to establish is that if 5 does not divide at least one of a or b then it does not divide $a^2 - 2b^2$. The squares modulo 5 are 0, 1 and 4, and multiplying by three we get 0, 3 and 2. If we take the sum of one number from the first list and

one number from the second, as before, the only way to get a number congruent to zero modulo 5, is to pick zero from both. The rest follows as in example 2.

8. Take I to be the set of all Gaussian integers of the form $a+bi$, where both a and b are divisible by 7. The key point is that if 7 does not divide a, then 7 does not divide $a^2 + b^2$. Indeed the squares modulo seven are 0, 1, 2 and 4, as can be seen by squaring 0, 1, 2 and 3 (for the rest observe that $a^2 = (-a)^2 = (7 - a)^2$, modulo seven). If a pair of these sum to a number divisible by 7, then both of these numbers must be 0. The rest follows as in example 2.