16.3 Prove Theorem 16.3. You can follow the outline below.

1. First observe that $r\bar{r}$ is a factorization of $N(r)$ in $\mathbb{Z}[i]$ as a product of Gaussian integers. Use the unique factoriztion theorem to deduce that every factorization of $N(r)$ in $\mathbb{Z}[i]$ as a product of irreducible Gaussian integers has two factors.

2. Observe that since r is not 0 or a unit in $\mathbb{Z}[i]$, its norm $N(r)$ is an integer greater than 1. Introduce notiation for a prime factorization of $N(r)$ is $\mathbb{Z}$, say $N(r) = p_1..p_t$. Be aware that the primes p_j may or may not be irreducible in $\mathbb{Z}[i]$; nothing is assumed about this. (Recall as an example that 2 is prime in $\mathbb{Z}$, but it is not irreducible in $\mathbb{Z}[i]$, since it factors as $2 = (1+i)(1-i)$. In any case, each prime p_j is a Gaussian integer ($p_j = p_j + 0i$), and therefore factors uniquely in $\mathbb{Z}[i]$ as a product of one or more Gaussian integers. ARgue that there must exist a factorization of $N(r)$ in $\mathbb{Z}[i]$ as a product of at least t irreducible Gaussian integers, and that therefore, by the first part, t equals 1 or 2.

3. Suppose that $t = 2$. Then $N(r) = r\bar{r} = p_1p_2$. Using the unique factorization theorem, deduce that r differs from either p_1 or p_2 by multiplication by a unit of $\mathbb{Z}[i]$. Conclude that there is a prime number p in $\mathbb{Z}$ such that r equals one of the four numbers $p, -p, pi, -pi$. Notice that in all four of these cases, $N(r) = p^2$

4. Suppose that $t = 1$. To simplify notation, write p_1 simply as p. Thus, $N(r) = p$. Write r as $a + bi$, for integers a, b. Observe that if either a, b is 0, then $N(r)$ cannot be a prime number. Thus, a, b are both nonzero. Observe that $p = N(r) = r\bar{r} = (a + bi)(a - bi) = a^2 + b^2$

16.6 Let us examine the two smallest rings of the form $\mathbb{Z}_m[i]$

1. According to the definitions, the ring $\mathbb{Z}_2[i]$ consists of all elements of the form $a+bi$, with $a, b \in \mathbb{Z}_2$. Deduce that $\mathbb{Z}_2[i]$ consists of four elements, $0, 1, i, 1+i$

2. Using these four elements, make addition and multiplication tables for $\mathbb{Z}_2[i]$, the way we did for fruit rings in Section 6.3

3. Review the multiplication table and answer the following questions:

a) Are there zero divisors in $\mathbb{Z}_2[i]$?

b) Does every nonzero element of $\mathbb{Z}_2[i]$ have a multiplicative inverse?

c) Is $\mathbb{Z}_2[i]$ a field?

4. Perform a similar analysis for the ring $\mathbb{Z}_3[i]$, starting with the observation that it contains nine distinct elements. List these elements, do not bother with the addition table, but make a multiplication table for $\mathbb{Z}_3[i]$. Use hte table to answer the following questions:

a) Are there zero divisors in $\mathbb{Z}_3[i]$?

b) Does every nonzero element of $\mathbb{Z}_3[i]$ have a multiplicative inverse?

c) Is $\mathbb{Z}_3[i]$ a field?

16.9 Prove theorem 16.9 by following the steps below:

1. Review the construction of the polynomial congruence rings in order to observe that the ring $\mathbb{F}_p[x]_{x^2+1}$ consists of elements of the form $c + d\gamma$ where c, d are in $\mathbb{F}_p$, the element γ satisfies the rule $\gamma^2 = -1$, and multiplication is given by the rule $(c + d\gamma)(e + f\gamma) = (ce - df) + (cf + de)\gamma$.

2. Compare this to the defining description of the ring $\mathbb{F}_p[i]$ given above. Notice that the descriptions are the same, except that we use γ in one case and i in the other.

3. Conclude that $\mathbb{F}_p[x]_{x^2+1}$ and $\mathbb{F}_p[i]$ are essentially the same rings; that is, they are identical except for a change in notation.

16.12 Prove theorem 16.15