Problem 1. Let $R = \mathbb{Z}[\sqrt{2}]$. Let p be a prime such that 2 is a quadratic residue modulo p so that $k^2 \equiv 2 \pmod{p}$ for some integer k. Let $I = pR = \{a + b\sqrt{2} : p|a, p|b\}$.

a) Prove that neither $k + \sqrt{2}$ nor $k - \sqrt{2}$ belong to I.

b) Use a) to prove that I is not a prime ideal.

Solution: a) This is obvious, since $a + b\sqrt{2} \in I$ iff $p|a$ and $b|b$. In our case $b = 1$ or $b = -1$, so $p \nmid b$.

b) Note that neither $k + \sqrt{2}$ nor $k - \sqrt{2}$ belong to I, yet

$$(k + \sqrt{2})(k - \sqrt{2}) = k^2 - 2 \in I$$

since $p|(k^2 - 2)$. Thus I is not a prime ideal.

Remark Similar argumet shows that if $\sqrt{n}$ is not rational and p is a prime such that n is a quadratic residue modulo p, then in the ring $R = \mathbb{Z}[\sqrt{n}]$ the ideal pR is not prime.

Problem 2. Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Let p be a prime number. Prove that pR is a maximal ideal iff -1 is a quadratic non-residue modulo p (i.e. iff $p \equiv 3 \pmod{4}$). (Follow the example we discussed for $\mathbb{Z}[\sqrt{2}]$. If you find it easier, prove that $2R$ is not prime and $7R$ is prime. But the general case is not much different.)

Solution: Suppose first that $p \equiv 1 \pmod{4}$ or $p = 2$ so -1 is a quadratic residue modulo p. Thus $k^2 \equiv -1 \pmod{p}$ for some integer k. Note that neither $k + i$ nor $k - i$ belong to pR but $(k + i)(k - i) = k^2 + 1 \in pR$ since $p|(k^2 + 1)$. Thus pR is not a prime ideal. Since every maximal ideal is prime, pR is not maximal.

Suppose now that $p \equiv 3 \pmod{4}$, so -1 is a quadratic non-residue modulo p.

Method I: We prove first that R/pR is an integral domain. Suppose that $[(a + bi) + pR][(c + di) + pR] = 0$ in R/pR. This means that $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in pR$, i.e. $p|ac - bd$ and $p|ad + bc$. In other words,

$$ac \equiv bd \pmod{p} \text{ and } ad \equiv -bc \pmod{p} . \quad (1)$$

Suppose first that p does not divide any of the integrs a, b, c, d. Then let us multiply the above congruences to get

$$a^2cd \equiv -b^2cd \pmod{p} \ , \text{ i.e. } p|(a^2+b^2)cd.$$

Since $p \nmid cd$, we get $p|a^2+b^2$. Thus $a^2 \equiv -b^2 \pmod{p}$. Multiplying this congruence by $(b^2)^{p-2}$ and using Fermat's Little Theorem we get

$$(ab^{p-2})^2 \equiv -(b^2)^{p-1} \equiv -1 \pmod{p}$$

which contradicts our assumption that -1 is a quadratic non-residue modulo p. Thus our assumption that none of the numbers a, b, c, d is divisible by p is wrong. At least one of these inetegrs is then divisible by p. Suppose that $p|a$ (the other 3 possibilities are handled similarly). If $p|b$ then $(a+bi)+I = 0+I$. Otherwise, from the congruences (1) we get $p|c$ and $p|d$, so $(c+di)+I = 0+I$.

We proved that if a product of two elements in R/pR is 0 then one of the factors is 0. This shows that R/pR is a domain. Note that R/pR is finite (has p^2 elements), so it is a field. Thus pR is a maximal ideal.

Method II: Suppose that pR is not maximal. Then there is a maximal ideal J which striclty contains pR. Thus R/J is a finite field. The number of elements in R/J is smaller than the number of elements in R/pR, which is p^2. On the other hand, since $p \in J$, the characteristic of R/J is p. By Problem 3 c) of homework 18, the number of elements in R/J is a power of p. The only power of p smaller than p^2 is p, so R/J has p elements. This means that it coincides with its subring $\mathbb{Z}/p$, i.e. we have a surjective homomorphism $f : R \longrightarrow \mathbb{Z}/p$. Let $x = f(i)$. Then

$$x^2 = f(i)^2 = f(i^2) = f(-1) = -f(1) = -1.$$

But our assumption about p means that -1 is not a square in $\mathbb{Z}/p$, a contradiction. This shows that pR is maximal.