Do the following exercises from Judson:
Section 16.6: 8, 13 (b)

8. Prove or Disprove: The ring $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a,\, b \in \mathbb{Q}\}$ is isomorphic to the ring $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a,\, b \in \mathbb{Q}\}$.

   ▶ **Solution.** The two rings are not isomorphic. To see this, suppose that $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ is a ring isomorphism and let $\phi(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Since a ring isomorphism will take the identity to the identity, we have

   $$2 = 1 + 1 = \phi(1) + \phi(1) = \phi(1 + 1) = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \phi(\sqrt{2})^2 = (a + b\sqrt{3})^2.$$

   Thus, $a^2 + 2ab\sqrt{3} + 3b^2 = 2$ and hence $2ab\sqrt{3} = 2 - a^2 - 3b^2$. If $ab \neq 0$ then

   $$\sqrt{3} = \frac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q}.$$

   If $ab = 0$ then $a = 0$ or $b = 0$. If $a = 0$ then $b^2 - \frac{2}{3}$ so $\sqrt{\frac{2}{3}} \in \mathbb{Q}$. If $b = 0$, then $2 = a^2$ and $\sqrt{2} \in \mathbb{Q}$. Since none of $\sqrt{2}$, $\sqrt{3}$, $\sqrt{\frac{2}{3}}$ are rational (by the same argument as the irrationality of $\sqrt{2}$), it follows that there can be no isomorphism ϕ between $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. ◀

13. (b) Solve the following system of congruences:

   $$\begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 0 \pmod{8} \\ x &\equiv 5 \pmod{15} \end{aligned}$$

   ▶ **Solution.** Since 7, 8, 15 are pairwise relatively prime, the Chinese Remainder theorem applies. Solve the first two congruences. Since $8 - 7 = 1$, $x = 3 \cdot 8 - 0 \cdot 7 = 24$ is the solution of the first two congruences modulo $8 \cdot 7 = 56$. Thus, the three congruences can be reduced to the pair of congruences

   $$\begin{aligned} x &\equiv 24 \pmod{56} \\ x &\equiv 5 \pmod{15} \end{aligned}$$

   From the Euclidian algorithm, $15^2 - 4 \cdot 56 = 1$. Thus, a solution of the last two congruences is $x = 24 \cdot 15^2 - 224 \cdot 5 = 4280 \pmod{840}$. The smallest positive solution is then $x \cong 80 \pmod{840}$. ◀

1. If F is a field and $|F| = q$, show that $a^q = a$ for all $a \in F$.

▶ **Solution.** Since F is a field, $F^* = F \setminus \{0\}$. Thus, F^* is a multiplicative group of order $q - 1$. Since the order of every element divides the order of the group, it follows that for all $a \neq 0$, $a^{q-1} = 1$. Multiplying by a gives $a^q = a$ for all $a \neq 0$. Since, it is also true that $0^q = 0$, it follows that $a^q = a$ for all $a \in F$. ◀

2. Show that $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} | m,\, n \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ and find 10 units.

▶ **Solution.** $0 = 0 + 0\sqrt{2}$ and $1 = 1 + 0\sqrt{2}$ are in $\mathbb{Z}(\sqrt{2})$. If $a = m + n\sqrt{2}$ and $b = p + q\sqrt{2}$ where $m,\, n,\, p,\, q \in \mathbb{Z}$ are typical element of $\mathbb{Z}(\sqrt{2})$ then $a \pm b = (m+n\sqrt{2}) \pm (p+q\sqrt{2}) = (m \pm q) + (n \pm q)\sqrt{2} \in \mathbb{Z}(\sqrt{2})$. Also, $ab = (m+n\sqrt{2})(p+q\sqrt{2}) = (mp + 2nq) + (np + mq)\sqrt{2} \in \mathbb{Z}(\sqrt{2})$. Thus, $\mathbb{Z}(\sqrt{2})$ is a subring of $\mathbb{C}$ by the subring test.

Assume that $u = m + n\sqrt{2} \in \mathbb{Z}(\sqrt{2})$. If $u^* = m - n\sqrt{2}$ then $uu^* = (m + n\sqrt{2})(m - n\sqrt{2}) = m^2 - 2n^2$. If $uu^* = \pm 1$ then u is a unit with $u^{-1} = \pm u^*$. Hence, find some choices of m and n by trial and error that satisfy $m^2 - 2n^2 = \pm 1$. Here are some examples: $m = \pm 1$, $n = 0$; $m = \pm 1$, $n = \pm 1$; $m = \pm 3$, $n = \pm 2$. These choices give the following units: ± 1, $\pm(1 \pm \sqrt{2})$, $\pm(3 \pm 2\sqrt{2})$. ◀

3. In each case decide whether A is an ideal of the ring R.

(a) $R = \mathbb{Z} \times \mathbb{Z}$, $A = \{(k,\, k) : k \in \mathbb{Z}\}$

▶ **Solution.** $a = (1,\, 1) \in A$ but if $r = (1,\, 0)$, then $ra = (1,\, 0)(1,\, 1) = (1,\, 0) \notin A$. Thus, A is not an ideal. ◀

(b) $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a,\, b,\, c \in \mathbb{Z} \right\}$, $A = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a,\, c \in \mathbb{Z},\, b \in 2\mathbb{Z} \right\}$.

▶ **Solution.** $a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in A$ but if $r = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, then $ar = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin A$. Thus, A is not an ideal. ◀

4. Let $R = \mathbb{Z}[i]$ be the ring of gaussian integers and let $A = R(1 + 3i) = \langle 1 + 3i \rangle$. Find the number of elements in the factor ring R/A and describe the cosets.

▶ **Solution.** Since $1 + 3i \in A$, so is $i(1 + 3i) = i - 3$. Thus, $i - 3 + A = 0 + A$ so $i + A = 3 + A$. Therefore $m + ni + A = m + 3n + A$ and hence every coset can be written as $k + A$ for $k \in \mathbb{Z}$. Since $10 = (1 + 3i)(1 - 3i) \in A$, it follows that $10 + A = 0 + A$. We claim that $R/A = \{k + A | 0 \leq k < 10\}$ and all of these cosets are distinct. To see this, we have already shown that $m + ni + A = (m + 3n) + A$. Divide $m + 3n$ by 10 in $\mathbb{Z}$ to get $m + 3n = 10q + k$ where $0 \leq k < 10$. Then,

$$m + ni + A = m + 3n + A = 10q + k + A = k + A$$

since $10 \in A$. It remains to show that all of the cosets $k + A$ for $0 \leq k < 10$ are all different. Suppose $k + A = j + A$ for $0 \leq k \leq j < 10$. Then $0 \leq j - k < 10$,

$j-k+A = 0+A$ and hence $j-k \in A$. Thus, $j-k = (1+3i)(r+si)$ for some r, $s \in \mathbb{Z}$. Multiplying out gives $j-k = (r-3s)+(3r+s)i$. Comparing real and imaginary terms gives

$$\begin{aligned} r-3s &= j-k \\ 3r+s &= 0. \end{aligned}$$

Multiplying the second equation by 3 and adding to the first gives $10r = j-k$, so that $j-k$ is a multiple of 10. Since, $1 \le j-k < 10$, it follows that $j-k = 0$ so that $j = k$. Hence, R/A consists of all the cosets $k+A$ for $0 \le k < 10$ and all of these cosets are distinct, so $|R/A| = 10$. ◀

5. Find all maximal ideals of (a) $\mathbb{Z}_8$, (b) $\mathbb{Z}_{10}$, (c) $\mathbb{Z}_{12}$, (d) $\mathbb{Z}_n$.

▶ **Solution.** All of the ideals of $\mathbb{Z}_n$ are $m\mathbb{Z}_n$ where m is a divisor of n. Thus, the ideals of $\mathbb{Z}_8$ are $\mathbb{Z}_8$, $2\mathbb{Z}_8$, $4\mathbb{Z}_8$ and $8\mathbb{Z}_8 = \{0\}$. These form a chain

$$\{0\} \subsetneqq 4\mathbb{Z}_8 \subsetneqq 2\mathbb{Z}_8 \subsetneqq \mathbb{Z}_8.$$

Thus, the only maximal ideal is $2\mathbb{Z}_8$.

Similarly for the other cases: the maximal ideals of $\mathbb{Z}_{10}$ are $2\mathbb{Z}_{10}$ and $5\mathbb{Z}_{10}$; the maximal ideals of $\mathbb{Z}_{12}$ are $2\mathbb{Z}_{12}$ and $3\mathbb{Z}_{12}$; the maximal ideals of $\mathbb{Z}_n$ are $p\mathbb{Z}_n$ where p is a prime divisor of n. ◀

6. (a) Show that $\mathbb{Z}_3[\sqrt{2}]$ is a field.

▶ **Solution.** This is like Example 5, Page 173. An argument like Example 4 shows that $\mathbb{Z}_3(\sqrt{2})$ is a ring. To show it is a field, it is necessary to show that every nonzero $a \in \mathbb{Z}_3(\sqrt{2})$ has a multiplicative inverse. The elements of $\mathbb{Z}_3(\sqrt{2})$ are $r + s\sqrt{2}$ where r and s are in $\mathbb{Z}_3$. Let $a = r + s\sqrt{2} \in \mathbb{Z}_3(\sqrt{2})$ and write $a^* = r - s\sqrt{2}$. Then $aa^* = r^2 - 2s^2 = r^2 + s^2 \in \mathbb{Z}_3$ since $-2 = 1 \in \mathbb{Z}_3$. If $a \ne 0$ then $r \ne 0$ or $s \ne 0$ in $\mathbb{Z}_3$. Thus $r^2 + s^2 \ne 0$ in $\mathbb{Z}_3$ since $t^2 = 0$ or 1 for all $t \in \mathbb{Z}_3$ and thus $r^2 + s^2$ can only be 1 or 2 if either $r \ne 0$ or $s \ne 0$. Letting $b = (r^2+s^2)^{-1}a*$ gives an element of $\mathbb{Z}(\sqrt{2})$ with $ab = 1 = ba$. Hence $\mathbb{Z}_3(\sqrt{2})$ is a field. ◀

(b) Show that $\mathbb{Z}_2[\sqrt{2}]$ has a unique proper ideal $A \ne 0$.

▶ **Solution.** The elements of $\mathbb{Z}_2(\sqrt{2})$ are $r + s\sqrt{2}$ where r, $s \in \mathbb{Z}_2$ so that there are 4 elements 0, 1, $\sqrt{2}$ and $1+\sqrt{2}$ where $\sqrt{2}$ is an element not in $\mathbb{Z}_2$ such that $(\sqrt{2})^2 = 2 = 0 \in \mathbb{Z}_2$. Thus, the multiplication table for $\mathbb{Z}_2(\sqrt{2})$ is

$\cdot$	0	1	$\sqrt{2}$	$1+\sqrt{2}$
0	0	0	0	0
1	0	1	$\sqrt{2}$	$1+\sqrt{2}$
$\sqrt{2}$	0	$\sqrt{2}$	0	$\sqrt{2}$
$1+\sqrt{2}$	0	$1+\sqrt{2}$	$\sqrt{2}$	1

The third row of this table shows that $A = \{0,\ \sqrt{2}\}$ is closed under multiplication by all elements of $\mathbb{Z}_2(\sqrt{2})$. It is also closed under addition. Hence it is a nonzero ideal. Moreover, 1 and $1 + \sqrt{2}$ are units, so any nonzero ideal, other than A will have a unit and hence will be all of $\mathbb{Z}_2(\sqrt{2})$. ◄

7. Show that $\mathbb{Z} \times 0$ and $0 \times \mathbb{Z}$ are prime ideals of $\mathbb{Z} \times \mathbb{Z}$. Are they maximal ideals?

   ► **Solution.** Let $\pi_1 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $\pi(r,\ s) = r$ and $\pi_2 : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $\pi_2(r,\ s) = s$. Both π_1 and π_2 are surjective ring homomorphisms. Thus, $\mathbb{Z} \times \mathbb{Z}/\operatorname{Ker}(\pi_i) \cong \mathbb{Z}$ for $i = 1,\ 2$. Hence, the kernel of each of these homomorphisms is a prime ideal, and $\operatorname{Ker}(\pi_1) = 0 \times \mathbb{Z}$ and $\operatorname{Ker}(\pi_2) = \mathbb{Z} \times 0$. So both of these ideals are prime. Neither is maximal since $0 \times \mathbb{Z} \subsetneqq (2\mathbb{Z}) \times \mathbb{Z} \subsetneqq \mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times 0 \subsetneqq \mathbb{Z} \times (2\mathbb{Z}) \subsetneqq \mathbb{Z} \times \mathbb{Z}$. ◄

8. The nonzero elements of $\mathbb{Z}_3[i]$ form an abelian group of order 8 (since $\mathbb{Z}_3[i]$ is a field). Determine the isomorphism class of this group.

   ► **Solution.** $1 - i$ is a nonzero element of $\mathbb{Z}_3[i]$, so the order of $1 - i$ is divisible by 8. Since $(1 - i)^2 = i$, $(1 - i)^4 = -1$, it follows that the order is not 1, 2, or 4. Hence the order must be 8, so the group is cyclic of order 8, and hence isomorphic to $\mathbb{Z}_8$. ◄