Exercise 13.4
Let $c = a + bi$ be a complex number with real coefficients. We can represent complex numbers on the 2-dimensional Cartesian plane by the point (a, b). Define the absolute value norm to be $|c| = \sqrt{a^2 + b^2}$, the Cartesian distance from the point (a, b) to the origin. In using this representation of complex numbers, we can write any complex number as the product of a real number r and a complex number $c = a + bi$ such that the norm of $|rc| = 1$. The absolute value product $|rc| = |r||c| = 1$:

$$|r| = \tfrac{1}{|c|}$$
$$|r| = \tfrac{1}{\sqrt{a^2+b^2}}$$
$$r = \tfrac{\sqrt{a^2+b^2}}{a^2+b^2}$$

Suppose the absolute value of c is 1. Then $\sqrt{a^2 + b^2} = 1$. Recall the trigonometric identity: $cos^2(\theta) + sin^2(\theta) = 1$ where θ is a real number. So,

$$\sqrt{cos^2(\theta) + sin^2(\theta)} = \sqrt{1} = 1$$
$$\sqrt{a^2 + b^2} = \sqrt{cos^2(\theta) + sin^2(\theta)}$$
$$a^2 = cos^2(\theta) \text{ and } b^2 = sin^2(\theta)$$
$$\text{Hence,}$$
$$a = cos(\theta) \text{ and } b = sin(\theta)$$

Therefore, $c = a + bi = cos(\theta) + isin(\theta)$. From the above results, we know that any complex number n can be written as the product of a real number r and a complex number. Then, $n = rc = r(cos(\theta) + isin(\theta))$.

Exercise 13.8: Determine which of the elements in the set $\mathbb{F}_p$ for $p = 3, 5, 7, 11, 13,$ and 19 are squares. The elements that have squares have been boxed.

Let $p = 3$

Element	Element Squared
0	0
$\boxed{1}$	1
2	1

There is 1 square

Let $p = 5$

Element	Element Squared
0	0
$\boxed{1}$	1
2	4
3	4
$\boxed{4}$	1

There are 2 squares

Let $p = 7$

Element	Element Squared
0	0
$\boxed{1}$	1
$\boxed{2}$	4
3	2
$\boxed{4}$	2
5	4
6	1

There are 3 squares

Let $p = 11$

Element	Element Squared
0	0
$\boxed{1}$	1
2	4
$\boxed{3}$	9
$\boxed{4}$	5
$\boxed{5}$	3
6	3
7	5
8	9
$\boxed{9}$	4
10	1

There are 5 squares

Let $p = 13$

Element	Element Squared
0	0
$\boxed{1}$	1
2	4
$\boxed{3}$	9
$\boxed{4}$	3
5	12
6	10
7	10
8	12
$\boxed{9}$	3
$\boxed{10}$	9
11	14
$\boxed{12}$	1

There are 6 squares

Let $p = 19$

Element	Element Squared
0	0
$\boxed{1}$	1
2	4
3	9
$\boxed{4}$	16
$\boxed{5}$	6
$\boxed{6}$	17
$\boxed{7}$	11
8	7
$\boxed{9}$	5
10	5
$\boxed{11}$	7
12	11
13	17
14	6
15	16
$\boxed{16}$	9
$\boxed{17}$	4
18	1

There are 9 squares

Exercise 13.12: For each of the prime numbers $p = 3, 5, 7, 11$, and 13, determine the orders of all the elements of $\mathbb{F}_p$.

Let $p = 3$

Element	Order
1	1
2	2

There is 1 element of order $p - 1 : \{2\}$

Let $p = 5$

Element	Order
1	1
2	4
3	4
4	2

There are 2 elements of order $p - 1 : \{2, 3\}$

Let $p = 7$

Element	Order
1	1
2	3
3	6
4	3
5	6
6	2

There are 2 elements of order $p - 1 : \{3, 5\}$

Let $p = 11$

Element	Order
1	1
2	10
3	5
4	5
5	5
6	10
7	10
8	10
9	5
10	2

There are 4 elements of order $p - 1 : \{2, 6, 7, 8\}$

Let $p = 13$

Element	Order
1	1
2	12
3	3
4	6
5	4
6	12
7	12
8	4
9	3
10	6
11	12
12	2

There are 4 elements of order $p - 1 : \{2, 6, 7, 11\}$

Exercise 13.16

Define K to be the set $K = \{a + b\gamma | a, b \in \mathbb{F}_3, \gamma^2 = 2\}$. Define addition and multiplication rules on K as follows:

$$(a + b\gamma) + (c + d\gamma) = (a + c) + (b + d)\gamma$$
$$\text{and}$$
$$(a + b\gamma)(c + d\gamma) = (ac + 2bd) + (ad + bc)\gamma$$

Observe that K is closed under addition and multiplication because $(a + c)$ mod 3 ,$(b + d)$ mod 3,$(ac + 2bd)$ mod 3, and $(ad + bc)$ mod 3 are all elements in $\mathbb{F}_3$. This means that K is a ring that contains the field $\mathbb{F}_3$. The following is a multiplication table of the 8 nonzero elements of K:

$\times$	1	2	$1+\gamma$	$1+2\gamma$	$2+\gamma$	$2+2\gamma$	γ	2γ
1	1	2	$1+\gamma$	$1+2\gamma$	$2+\gamma$	$2+2\gamma$	γ	2γ
2	2	1	$2+2\gamma$	$2+\gamma$	$1+2\gamma$	$1+\gamma$	2γ	γ
$1+\gamma$	$1+\gamma$	$2+2\gamma$	2γ	2	1	γ	$2+\gamma$	2
$1+2\gamma$	$1+2\gamma$	$2+\gamma$	2	γ	2γ	1	$1+\gamma$	$2+2\gamma$
$2+\gamma$	$2+\gamma$	$1+2\gamma$	1	2γ	γ	2	$2+2\gamma$	$1+\gamma$
$2+2\gamma$	$2+2\gamma$	$1+\gamma$	γ	1	2	2γ	$1+\gamma$	$2+\gamma$
γ	γ	2γ	$2+\gamma$	$1+\gamma$	$2+2\gamma$	$1+\gamma$	2	1
2γ	2γ	γ	2	$2+2\gamma$	$1+\gamma$	$2+\gamma$	1	2

Notice that every non-zero element has a multiplicative inverse such that $(a + b\gamma)(a + b\gamma)^{-1} = 1$. Therefore, K is a field. Observe that

$$(a + b\gamma)(a - b\gamma) = a^2 - ab\gamma + ab\gamma - b^2\gamma^2$$
$$a^2 - 2b^2$$
$$a^2 + b^2 \text{ mod } 3$$

Consider the possible values for $a^2 + b^2$ in $\mathbb{F}_3$:

$$(a, b) = (0, 0), a^2 + b^2 = 0$$
$$(a, b) = (0, 1), a^2 + b^2 = 1$$
$$(a, b) = (0, 2), a^2 + b^2 = 4 = 1$$
$$(a, b) = (1, 0), a^2 + b^2 = 1$$
$$(a, b) = (2, 0), a^2 + b^2 = 4 = 1$$
$$(a, b) = (1, 1), a^2 + b^2 = 2$$
$$(a, b) = (1, 2), a^2 + b^2 = 5 = 2$$
$$(a, b) = (2, 1), a^2 + b^2 = 5 = 2$$
$$(a, b) = (2, 2), a^2 + b^2 = 8 = 2$$

Notice that the only time $a^2 + b^2 = 0$ is when $a = b = 0$. Assume that a and b are not zero, so $a^2 + b^2 \neq 0$. Because $a^2 + b^2$ is not zero and $\mathbb{F}_3$ is a field, $a^2 + b^2$ has an inverse, call it $(a^2 + b^2)^{-1}$. Now, we can perform the following operation:

$$
\begin{gathered}
(a + b\gamma)(a - b\gamma)/(a^2 + b^2) \\
(a + b\gamma)(a - b\gamma)(a^2 + b^2)^{-1} \\
(a + b\gamma)[a(a^2 + b^2)^{-1} - b\gamma(a^2 + b^2)^{-1}] \\
(a^2 + ab\gamma)(a^2 + b^2)^{-1} - (ab\gamma + b^2\gamma^2)(a^2 + b^2)^{-1} \\
(a^2 - 2b^2)(a^2 + b^2)^{-1} \\
(a^2 + b^2)(a^2 + b^2)^{-1} = 1
\end{gathered}
$$

Hence, for all elements of K, $a + b\gamma$, its inverse exists so we have confirmed that K is a field. Notice that if $f(x) = x^2 - 2$, $f(\gamma) = \gamma^2 - 2 = 2 - 2 = 0$, so $f(x)$ has a root in K and factors as $f(x) = (x + \gamma)(x - \gamma)$ in $K[x]$.

Since K is a field with 9 elements, we will rename it $\mathbb{F}_9$ instead. By theorem 13.9 in the textbook, $\mathbb{F}_9$ has a primitive root. Observe:

$$
\begin{gathered}
(1 + \gamma)^1 = 1 + \gamma \\
(1 + \gamma)^2 = 2\gamma \\
(1 + \gamma)^3 = 1 + 2\gamma \\
(1 + \gamma)^4 = 2 \\
(1 + \gamma)^5 = 2 + 2\gamma \\
(1 + \gamma)^6 = \gamma \\
(1 + \gamma)^7 = 2 + \gamma \\
(1 + \gamma)^8 = 1
\end{gathered}
$$

Therefore, $1 + \gamma$ is a primitive root because $(1 + \gamma)^k = \mathbb{F}_9^\times$ for $0 < k < 9$.

Exercise 13.20
Let p be an odd prime and let α be a primitive root in the field $\mathbb{F}_p$ such that $\mathbb{F}_p^\times = \{\alpha, \alpha^2, \alpha^3, ...\alpha^{p-1}\}$, where $\sqrt{\alpha}$ is not an element of $\mathbb{F}_p$. We will construct a new set $\mathbb{F}_p[\sqrt{\alpha}] = \{a + b\sqrt{\alpha} | a, b \in \mathbb{F}_p, \sqrt{\alpha} \notin \mathbb{F}_p\}$. Define addition and multiplication rules on $\mathbb{F}_p[\sqrt{a}]$ to be as follows:

$$(a + b\sqrt{\alpha}) + (c + d\sqrt{\alpha}) = (a + c) + (b + d)\sqrt{\alpha}$$
and
$$(a + b\sqrt{\alpha})(c + d\sqrt{\alpha}) = (ac + bd\alpha) + (ad + bc)\sqrt{\alpha}$$

Observe that $\mathbb{F}_p[\sqrt{\alpha}]$ is closed under addition and multiplication because $(a + c) \bmod p$,$(b + d) \bmod p$,$(ac + bd\alpha) \bmod p$, and $(ad + bc) \bmod p$ are all elements in $\mathbb{F}_p$. This means that $\mathbb{F}_p[\sqrt{\alpha}]$ is a ring that contains the field $\mathbb{F}_p$ and where the square of α exists. Because $\mathbb{F}_p$ has p elements, for each element $a + b\sqrt{\alpha}$ in $\mathbb{F}_p[\sqrt{\alpha}]$, there are p choices for a and p choices for b, so $\mathbb{F}_p[\sqrt{\alpha}]$ has p^2 elements, including the zero element.

To show that every element of $\mathbb{F}_p[\alpha]$ has a square, we will begin by proving that $\mathbb{F}_p[\alpha]$ is a field. Observe that

$$\begin{aligned}(a + b\sqrt{\alpha})(a - b\sqrt{\alpha}) &= a^2 - ab\sqrt{\alpha} + ba\sqrt{\alpha} + \alpha b^2 \\ &= a^2 - \alpha b^2\end{aligned}$$

Lemma: If $a + b\sqrt{\alpha} \neq 0$, then $a^2 - \alpha b^2 \neq 0$.
Proof: Suppose instead that $a^2 - \alpha b^2 = 0$. Then

$$\begin{gathered}a^2 = \alpha b^2 \\ a^2(b^{-1})^2 = \alpha \\ (ab^{-1})^2 = \alpha \\ ab^{-1} = \sqrt{\alpha}\end{gathered}$$

This implies $\sqrt{\alpha} \in \mathbb{F}_p$ since ab^{-1} exists in the field $\mathbb{F}_p$. Then, this is a contradtion because $\sqrt{\alpha} \notin \mathbb{F}_p$. Therefore, by proof of contradiction, if $a + b\sqrt{\alpha} \neq 0$, then $a^2 - \alpha b^2 \neq 0$. $\square$

Now, given $a + b\sqrt{\alpha} \neq 0$, we know that $a^2 - \alpha b^2 \neq 0$. Recall that

$$(a + b\sqrt{\alpha})(a - b\sqrt{\alpha}) = a^2 - \alpha b^2$$

We can divide the product $(a+b\sqrt{\alpha})(a-b\sqrt{\alpha})$ by $a^2-\alpha b^2$ because $a^2-\alpha b^2 \neq 0$ so its inverse exsists in $\mathbb{F}_p$. The inverse of $a^2-\alpha b^2$ will be given by $(a^2-\alpha b^2)^{-1}$. Hence:

$$
\begin{gathered}
(a+b\sqrt{\alpha})(a-b\sqrt{\alpha})/(a^2-\alpha b^2) \\
(a+b\sqrt{\alpha})(a-b\sqrt{\alpha})(a^2-\alpha b^2)^{-1} \\
(a+b\sqrt{\alpha})[a(a^2-\alpha b^2)^{-1}-\alpha b^2(a^2-\alpha b^2)^{-1}] \\
(a^2+ab\sqrt{\alpha})(a^2-\alpha b^2)^{-1}-(ab\sqrt{\alpha}+\alpha b^2)(a^2-\alpha b^2)^{-1} \\
(a^2+ab\sqrt{\alpha}-ab\sqrt{\alpha}+\alpha b^2)(a^2-\alpha b^2)^{-1} \\
(a^2-\alpha b^2)(a^2-\alpha b^2)^{-1}=1
\end{gathered}
$$

Therefore, for all non-zero elements in $\mathbb{F}_p[\sqrt{\alpha}]$, $a+b\sqrt{\alpha}$, the inverse exists so $\mathbb{F}_p[\sqrt{\alpha}]$ is a field.

In conclusion, we began with a field $\mathbb{F}_p$ which has a primitive root α such that $\mathbb{F}_p^\times = \{\alpha, \alpha^2, \alpha^3, ...\alpha^{p-1}\}$, but, $\sqrt{\alpha}$ did not exist in $\mathbb{F}_p$. Then, we created a new field $\mathbb{F}_p[\sqrt{\alpha}]$ where the square of α existed. Since α is a primitave root, for all $k \in \mathbb{F}_p^\times$, there exists an integer $m \leq p-1$ such that $\alpha^m = k$ and thus $\sqrt{k} = \sqrt{\alpha^m} = (\sqrt{\alpha})^m$ which we have proven exists. This means that every non zero element of $\mathbb{F}_p$ has a square. Therefore, for all numbers $b, c \in \mathbb{F}_p$, the polynomial $f(x) = x^2 + bx + c$ has roots in $\mathbb{F}_p[\sqrt{\alpha}]$ because its discriminant $\sqrt{b^2 - 4c}$ exists. $\square$