Throughout, \( \mathbb{N} \) (resp., \( \mathbb{Z} \)) denotes the set of positive integers (resp., all integers). The notation \( a \mid b \) is to be read “\( a \) divides \( b \).” By “prime number,” we always mean “positive prime number.” For all \( m \in \mathbb{Z} \), we write \( U_m \) to denote the group \((\mathbb{Z}/m\mathbb{Z})^\times\) of units modulo \( m \).

Exercise 6.1

Find the orders of the elements of \( U_9 \) and \( U_{10} \).

Note that \( \varphi(9) = 6 \) and \( \varphi(10) = 4 \). We see \([2]_9\) generates \( U_9 \) and its first 6 powers, in order, are represented by \( 2, 4, 8, 7, 5, 1 \). So the orders of the elements of \( U_9 \) are:

\[
\begin{array}{c|cccccc}
 n & 2 & 4 & 8 & 7 & 5 & 1 \\
\text{ord}([n]_9) & 6 & 3 & 2 & 3 & 6 & 1 \\
\end{array}
\]

We see \([3]_{10}\) generates \( U_{10} \) and its first 4 powers, in order, are represented by \( 3, 9, 7, 1 \). So the orders of the elements of \( U_{10} \) are:

\[
\begin{array}{c|cccc}
 n & 3 & 9 & 7 & 1 \\
\text{ord}([n]_{10}) & 4 & 2 & 4 & 1 \\
\end{array}
\]

Exercise 6.2

Show that if \( \ell, m \in \mathbb{N} \) and \( h = \gcd(\ell, m) \), then \( \gcd(2^{\ell} - 1, 2^m - 1) \) divides \( 2^h - 1 \).

Let \( d = \gcd(2^\ell - 1, 2^m - 1) \), so that \( 2 \in U_d \) by the oddness of \( d \). We have \( 2^\ell \equiv 1 \equiv 2^m \) \( (\mod d) \), so \( 2^{\ell x + my} \equiv 1 \) \( (\mod d) \) for all \( x, y \in \mathbb{Z} \). By Bézout’s Theorem, we can pick \( x, y \) such that \( \ell x + my = h \). Therefore, \( 2^h \equiv 1 \) \( (\mod d) \), i.e., \( d \) divides \( 2^h - 1 \).

Exercise 6.3

The groups \( U_{10}, U_{12} \) both have order 4. Show that exactly one of them is cyclic.

Our work on [JJ, Ex. 6.1] showed that \( U_{10} \) was generated by \([3]_{10}\), hence cyclic. By contrast, a full set of representatives for \( U_{12} \) is \( \{1, 5, 7, 11\} \) and \( 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \) \( (\mod 12) \), so \( U_{12} \) cannot be cyclic.

Exercise 6.4

Find primitive roots in \( U_n \) for \( n = 18, 23, 27, 31 \).

Possible primitive roots for \( U_{18}, U_{23}, U_{27}, U_{31} \) are 5, 5, 2, 3, respectively, according to [JJ]; to check that these work, one can verify that their orders are the orders of the respective groups: \( \varphi(18) = 6, \varphi(23) = 22, \varphi(27) = 18, \varphi(31) = 30 \).
**Exercise 6.5**

Show that if $U_n$ has a primitive root, then it has $\phi(\phi(n))$ of them.

**Lemma 1.** $[a]_m$ generates $\mathbb{Z}/m\mathbb{Z}$ if and only if $a$ is coprime to $m$.

**Proof.** By Bézout’s Theorem, $[a]_m$ generates precisely the subgroup $\gcd(a, m)\mathbb{Z}/m\mathbb{Z}$ of $\mathbb{Z}/m\mathbb{Z}$. \[\square\]

If $U_n$ has a primitive root, then it is isomorphic to the cyclic group of order $\#U_n = \phi(n)$, i.e., to the additive group $\mathbb{Z}/\phi(n)\mathbb{Z}$. But by the lemma above, $\mathbb{Z}/m\mathbb{Z}$ has precisely $\phi(m)$ generators for all $m \in \mathbb{N}$; taking $m = \phi(n)$ gives the result.

**Exercise 6.6**

Verify that 5 is a generator of $U_7$.

We see $\#U_7 = \phi(7) = 6$ and the first 6 powers of $[5]_7$, in order, are represented by 5, 4, 6, 2, 3, 1, which proves that the order of 5 is $\#U_7$, as needed.

**Exercise 6.7**

For each $d \mid 10$, find all the elements of $U_{11}$ of order $d$. Which are the generators?

We observe that 2 is a generator of $U_{11}$, as its first 10 powers, in order, are represented by 2, 4, 8, 5, 10, 9, 7, 3, 6, 1. Thus the orders of these elements are:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\text{ord}([n]_{11})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

To get the table above, we used Bézout’s Theorem to infer that $[2^k]_{11}$ generates the cyclic subgroup of $U_{11}$ that corresponds to $\gcd(k, 10)\mathbb{Z}/10\mathbb{Z}$ under the isomorphism $U_{11} \simeq \mathbb{Z}/10\mathbb{Z}$. In particular, the generators are represented by 2, 8, 7, 6, as these correspond to $2^1, 2^3, 2^7, 2^9$, respectively; cf. Lem. 1.

**Exercise 6.9**

Show that 2 is a primitive root modulo $3^e$ for all $e \geq 1$.

We can check that 2 represents a primitive root modulo $3^2$. Using claim (c) on [JJ, 104], which is part of the proof of [JJ, Thm. 6.7], this fact implies that 2 represents a primitive root modulo $3^e$ for all $e \geq 1$.

**Exercise 6.10**

Find an integer that is a primitive root modulo $7^e$ for all $e \geq 1$.

We compute $3^6 \equiv 729 \equiv 43 \not\equiv 1 \pmod{7^2}$. Hence, under the isomorphism

$$U_{7^2} \to \mathbb{Z}/\phi(7^2)\mathbb{Z} \simeq \mathbb{Z}/42\mathbb{Z},$$

the element $[3]_{7^2}$ corresponds to a residue $[a]_{42}$ such that $6a \not\equiv 0 \pmod{42}$, i.e., such that $a \not\equiv 0 \pmod{7}$. At the same time, we compute that 3 represents a primitive root modulo 7. Hence, under the isomorphism

$$U_7 \to \mathbb{Z}/\phi(7)\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z},$$

the element $[3]_7$ corresponds to a generator of $\mathbb{Z}/6\mathbb{Z}$, i.e., to a residue coprime to 6. But the isomorphisms (4) and (5) commute with the reduction maps $U_{7^2} \to U_7$ and $\mathbb{Z}/42\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, in the sense that the image of $[3]_7$ in $\mathbb{Z}/6\mathbb{Z}$ must be the same as the image of $[a]_{42}$ in $\mathbb{Z}/6\mathbb{Z}$. We
deduce that $a$ is coprime to 6. Our earlier work showed it is coprime to 7. Therefore, $[a]_{42}$ is a generator of the additive group $\mathbb{Z}/42\mathbb{Z}$, which means, via the isomorphism $\mathbb{Z}/42\mathbb{Z} \cong \mathbb{U}_{72}$, that $[3]_{72}$ is a generator of $\mathbb{U}_{72}$. Just as in Exercise 6.9, [3], 104 lets us conclude that 3 represents a primitive root modulo $7^e$ for all $e \geq 1$.

**Exercise 2**

Check that 3 is a primitive root modulo 17 by constructing an explicit isomorphism $\mathbb{Z}/16\mathbb{Z} \to \mathbb{U}_{17}$ that sends $[1]_{16} \mapsto [3]_{17}$. Using this map, solve:

1. $z^{12} \equiv 16 \pmod{17}$.
2. $z^{20} \equiv 13 \pmod{17}$.
3. $z^{48} \equiv 9 \pmod{17}$.
4. $z^{11} \equiv 9 \pmod{17}$.

Since $\mathbb{Z}/16\mathbb{Z}$ is cyclic, being additively generated by $[1]_{16}$, any group homomorphism $\psi : \mathbb{Z}/16\mathbb{Z} \to \mathbb{U}_{17}$ is completely determined by the image of $[1]_{16}$: It must satisfy

$$\psi([n]_{16}) = \psi([1]_{16})^n.$$  

In particular, if $\psi([1]_{16}) = [3]_{17}$, then $\psi$ must be given by the following table:

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi([n])$</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>10</td>
<td>13</td>
<td>5</td>
<td>15</td>
<td>11</td>
<td>16</td>
<td>14</td>
<td>8</td>
<td>7</td>
<td>4</td>
<td>12</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

To solve a congruence of the form $z^n \equiv a \pmod{17}$ for $[z]_{17}$ using this table: Applying $\psi^{-1}$ to both sides, we obtain $n\psi^{-1}(z) \equiv \psi^{-1}(a) \pmod{16}$. After solving this linear congruence for $\psi^{-1}(z)$, we can apply $\psi$ to recover $z$. Thus, for the cases listed:

1. $12\psi^{-1}(z) \equiv 8 \pmod{16}$. Dividing through by 4, we have $3\psi^{-1}(z) \equiv 2 \pmod{4}$, giving $\psi^{-1}(z) \equiv 2 \pmod{4}$. Therefore, $\psi^{-1}(z) \equiv 2, 6, 10, 14 \pmod{16}$, whence $z \equiv 9, 15, 8, 2 \pmod{17}$.
2. $20\psi^{-1}(z) \equiv 4 \pmod{16}$. Dividing through by 4, we have $\psi^{-1}(z) \equiv 5\psi^{-1}(z) \equiv 1 \pmod{4}$. Therefore, $\psi^{-1}(z) \equiv 1, 5, 9, 13 \pmod{16}$, whence $z \equiv 3, 5, 14, 12 \pmod{17}$.
3. $48\psi^{-1}(z) \equiv 2 \pmod{16}$. Dividing through by 2, we have $24\psi^{-1}(z) \equiv 1 \pmod{8}$, which has no solutions because $24\psi^{-1}(z) \equiv 0 \psi^{-1}(z) \equiv 0 \pmod{8}$. So there are no solutions for $z$.
4. $11\psi^{-1}(z) \equiv 2 \pmod{16}$. Since $3 \cdot 11 \equiv 33 \equiv 1 \pmod{16}$, we get $\psi^{-1}(z) \equiv 3 \cdot 11 \psi^{-1}(z) \equiv 3 \cdot 2 \equiv 6 \pmod{16}$, from which $z \equiv 15 \pmod{17}$.

**Exercise 7.1**

Find all solutions of $x^2 - 3x + 2 \equiv 0 \pmod{15}$.

The discriminant of the quadratic polynomial $ax^2 + bx + c = x^2 - 3x + 2$ is

$$\Delta = b^2 - 4ac = (-3)^2 - 4(1)(2) = 1,$$

which, modulo 15, has the square roots $[\pm 1]_{15}$. Therefore, by the quadratic formula, the solutions to the given congruence satisfy

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-(-3) \pm 1}{2(1)} \pmod{15},$$

where the division in the second and third expressions is to be interpreted as multiplication by the inverse of $2a = 2(1)$ in $\mathbb{Z}/15\mathbb{Z}$. This inverse is 8, so we get $x \equiv (-(-3) \pm 1) \cdot 8 \equiv 16, 32 \equiv 1, 2 \pmod{15}$. 
Exercise 7.2

What square roots do the elements 5 and 16 have in \( \mathbb{Z}/21\mathbb{Z} \)? From this, find all solutions to the congruences \( x^2 + 3x + 1 \equiv 0 \pmod{21} \) and \( x^2 + 2x - 3 \equiv 0 \pmod{21} \).

There are no solutions to \( x^2 + 3x + 1 \equiv 0 \pmod{21} \), because there are no solutions to \( x^2 + 1 \equiv x^2 + 3x + 1 \equiv 0 \pmod{3} \). In particular, there cannot exist square roots of the residue of 5 in \( \mathbb{Z}/21\mathbb{Z} \), because \([5]_{21}\) is the discriminant of \( x^2 + 3x + 1 \) modulo 21.

To compute the square roots of the residue of 16 in \( \mathbb{Z}/21\mathbb{Z} \), it suffices by the Chinese Remainder Theorem to compute the square roots in the rings \( \mathbb{Z}/3\mathbb{Z} \) and \( \mathbb{Z}/7\mathbb{Z} \), then find the residues in \( \mathbb{Z}/21\mathbb{Z} \) that are “lifts” of square roots from both of these rings simultaneously. Explicitly:

\[
(\pm 1)^2 \equiv 16 \pmod{3},
\]

\[
(\pm 4)^2 \equiv 16 \pmod{7};
\]

solving the system of linear congruences

\[
\begin{aligned}
& s \equiv \pm 1 \pmod{3} \\
& s \equiv \pm 4 \pmod{7}
\end{aligned}
\]

yields \( s \equiv \pm 4, \pm 10 \pmod{21} \). Now, \([16]_{21}\) is the discriminant of \( ax^2 + bx + c = x^2 + 2x - 3 \) modulo 21, so altogether, by the quadratic formula, the solutions to \( x^2 + 2x - 3 \equiv 0 \pmod{21} \) are

\[
x \equiv \frac{-b \pm s}{2a} \equiv \frac{-2 \pm s}{2(1)} \pmod{21}.
\]

As in Exercise 7.1, the division by \( 2a = 2(1) \) above is defined to be multiplication by its inverse in \( \mathbb{Z}/21\mathbb{Z} \), i.e., multiplication by 11. Therefore,

\[
(14) \quad x \equiv (-2 \pm 4)(11), (-2 \pm 10)(11) \equiv -3, 1, 4, 15 \pmod{21}.
\]

Reference