Ch. 19, 21, and 22
Defn: Let \( m \in \mathbb{Z} \). Two integers \( a \) and \( b \) are congruent modulo \( m \), written \( a \equiv b \mod m \), if \( a-b \) is divisible by \( m \) (there is \( q \in \mathbb{Z} \) with \( a-b=qn \)).

Ex: \( 14 \equiv 2 \mod 3 \) because 3 divides 12 and 12 = 14 - 2.

Prop: Let \( m \in \mathbb{Z} \). Congruence modulo \( m \) has the following three properties:

1. Reflexive property: \( a \equiv a \mod m \) for all integers \( a \).
2. Symmetric property: If \( a \equiv b \mod m \) then \( b \equiv a \mod m \).
3. Transitive property: If \( a \equiv b \mod m \) and \( b \equiv c \mod m \) then \( a \equiv c \mod m \).

Proof:

1. \( a-a = 0 = 0 \cdot m \) so \( a \equiv a \mod m \).
2. If \( a \equiv b \mod m \) then there is \( q \in \mathbb{Z} \) with \( a-b=qn \). Then \( b-a = (-q)m \) and therefore \( b \equiv a \mod m \).
3. Assume \( a \equiv b \mod m \) and \( b \equiv c \mod m \). Then there are \( p,q \in \mathbb{Z} \) with \( a-b = pm \) and \( b-c = qm \). So \( a-c = (a-b)+(b-c) = pm+qm = (p+q)m \) and therefore \( a \equiv c \mod m \).

Congruence modulo \( m \) is an example of an equivalence relation.

Defn: Let \( X \) be a set and let \( \sim \) be a relation between elements of \( X \). We call \( \sim \) an equivalence relation if it has the properties of being reflexive, symmetric, and transitive. (This is described more precisely in Definition 22.2.3 in your book.)
Defn: Let \( a \in \mathbb{Z} \). The congruence class of \( a \) modulo \( m \), denoted \([a]_m\), is the set of integers that are congruent to \( a \) modulo \( m \):
\[
[a]_m = \{ b \in \mathbb{Z} : b \equiv a \mod m \}
\]

Example:
\[
[0]_3 = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}
\]
\[
[1]_3 = \{ \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \}
\]
\[
[2]_3 = \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}
\]

Let \( m \in \mathbb{Z} \). By the division theorem, for every \( a \in \mathbb{Z} \) there is a unique \( r \in \mathbb{Z} \) with \( 0 \leq r < m \) and such that \( \exists q \in \mathbb{Z} \) \( a = qm + r \). This means that for every \( a \in \mathbb{Z} \) there is precisely one integer \( r \), \( 0 \leq r < m \), so that \( a \equiv r \mod m \). (In other words, for every \( a \in \mathbb{Z} \) there is precisely one integer \( r \) with \( 0 \leq r < m \) and \( a \in [r]_m \).

The collection \( \{ [0]_m, [1]_m, [2]_m, \ldots, [m-1]_m \} \) is an example of a partition.

Defn: A collection \( \mathcal{X} = \{ Y_1, Y_2, \ldots, Y_n \} \) is a partition of \( X \) if each \( Y_i \) is a non-empty subset of \( X \) and if for every \( x \in X \) there is precisely one \( i \) \( (1 \leq i \leq n) \) with \( x \in Y_i \).

We write \( \mathbb{Z}_m \) for the collection \( \{ [0]_m, [1]_m, \ldots, [m-1]_m \} \).
Prop: Let \( a, a_2, b, b_2, m \in \mathbb{Z} \). Assume that
\[
a_1 \equiv a_2 \mod m \quad \text{and} \quad b_1 \equiv b_2 \mod m.
\]
Then
1. \( a_1 + b_1 \equiv a_2 + b_2 \mod m \)
2. \( a_1 - b_1 \equiv a_2 - b_2 \mod m \)
3. \( a_1 b_1 \equiv a_2 b_2 \mod m \)

Proof: Let \( p, q \in \mathbb{Z} \) with \( a_1 - a_2 = pm \) and \( b_1 - b_2 = qm \).
1. \( (a_1 + b_1) - (a_2 + b_2) = a_1 - a_2 + b_1 - b_2 = pm + qm = (p+q)m \)
   so \( a_1 + b_1 \equiv a_2 + b_2 \mod m \)
2. similar to 1 (exercise)
3. \( a_1 b_1 - a_2 b_2 = (a_1 b_1 - a_2 b_1) + (a_2 b_1 - a_2 b_2) \)
   \[= (a_1 - a_2)b_1 + (b_1 - b_2)a_2 \]
   \[= b_1 pm + a_2 qm \]
   \[= (b_1 p + a_2 q)m \]
so \( a_1 b_1 \equiv a_2 b_2 \mod m \). \( \square \)

Example: For any integer \( n \geq 1 \), since \( 4 \equiv 1 \mod 3 \) we have
\[4^n + 5 \equiv 1^n + 2 \equiv 1 + 2 \equiv 0 \mod 3, \]
so 3 divides \( 4^n + 5 \) (we previously proved this using induction on \( n \)).

The above proposition tells us that we can make sense of addition, subtraction, and multiplication on the set \( \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\} \). This is similar to statements such as the product of two odd numbers is odd.

When \( m = 3 \), addition and multiplication are given as follows:

<table>
<thead>
<tr>
<th>+</th>
<th>[0]_3</th>
<th>[1]_3</th>
<th>[2]_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]_3</td>
<td>[0]_3</td>
<td>[1]_3</td>
<td>[2]_3</td>
</tr>
<tr>
<td>[1]_3</td>
<td>[1]_3</td>
<td>[2]_3</td>
<td>[0]_3</td>
</tr>
<tr>
<td>[2]_3</td>
<td>[2]_3</td>
<td>[0]_3</td>
<td>[1]_3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x</th>
<th>[0]_3</th>
<th>[1]_3</th>
<th>[2]_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]_3</td>
<td>[0]_3</td>
<td>[0]_3</td>
<td>[0]_3</td>
</tr>
<tr>
<td>[1]_3</td>
<td>[0]_3</td>
<td>[1]_3</td>
<td>[2]_3</td>
</tr>
<tr>
<td>[2]_3</td>
<td>[2]_3</td>
<td>[0]_3</td>
<td>[1]_3</td>
</tr>
</tbody>
</table>