We were proving:

**Basic Properties of Congruence Arithmetic.**

1. \(a \equiv a \pmod{n}; \quad a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}; \)
   \[
   \begin{align*}
   a & \equiv b \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}, \\
   b & \equiv c \pmod{n} 
   \end{align*}
   \]

2. \(a_1 \equiv a_2 \pmod{n} \quad \Rightarrow \quad a_1 + b_1 \equiv a_2 + b_2 \pmod{n}; \quad b_1 \equiv b_2 \pmod{n} \)

3. \(a_1 \equiv a_2 \pmod{n} \quad \Rightarrow \quad a_1 b_1 \equiv a_2 b_2 \pmod{n}; \quad b_1 \equiv b_2 \pmod{n} \)

4. \(a \equiv r \pmod{n} \) and \(0 \leq r < n \quad \iff \) \(r \) is the remainder of \(a\) divided by \(n\).

If (3) (continue) \(a_1 - a_2 = nk, \ b_1 - b_2 = nl \) for some \(k, l \in \mathbb{Z}\).

\[
\begin{align*}
    a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2 \\
                    &= (a_1 - a_2) b_1 + a_2 (b_1 - b_2) \\
                    &= nk b_1 + a_2 n l \\
                    &= n (k b_1 + a_2 l) \\
                    &\in \mathbb{Z}
\end{align*}
\]

\(a_1 b_1 \equiv a_2 b_2 \pmod{n} \).

(4) (\(\Rightarrow\)) By definition, \(r \in \{0, 1, \ldots, n-1\} \) and \(a = nq + r\).

And so \(n \mid a - r\); therefore \(a \equiv r \pmod{n}\).

(\(\Leftarrow\)) Suppose \(r \in \{0, 1, \ldots, n-1\} \) and \(a \equiv r \pmod{n}\). Then
$\exists q \in \mathbb{Z} \text{ s.t. } a - r = nq$. Therefore

(1) $a = nq + r$  \hspace{1cm} (2) $0 \leq r < n$. Thus, by the uniqueness part of the division algorithm, $r$ is the remainder of $a$ divided by $n$. ■

Ex. Let $n = 124567932$. Find the remainder of $n$ divided by 9. What is the remainder of $n$ divided by 11?

**Solution.** First we prove by induction on $m$ that

$10^m = 1 \pmod{9}$ and $10^m = (-1)^m \pmod{11}$.

**Base of induction.** $10^0 = 1 \equiv (1)^0 \pmod{9}$ and $10^0 = 1 \equiv (1)^0 \pmod{11}$.

**Induction step.** $10^{m+1} = (10^m)(10) \equiv (1)(1) \pmod{9}$

(by induction hypothesis)

$10^m = 1 \pmod{9}$ and $10 \equiv 1 \pmod{9}$

$10^{m+1} = (10^m)(10) \equiv (-1)^m (-1) \pmod{11}$

(by induction hypothesis)

$10^m \equiv -1 \pmod{11}$

$10 \equiv -1 \pmod{11}$
Just adding its digits:

$$124567932 = 1 + 2 + 4 + 5 + 6 + 7 + 9 + 3 + 2 = 3 \pmod{9}, \text{ and so the remainder of } n \text{ divided by } 9 \text{ is } 3.$$

Alternate signs and digits:

$$124567932 = (-1)^8 \times 1 + (-1)^7 \times 2 + (-1)^6 \times 4 + (-1)^5 \times 5 + (-1)^4 \times 6 + (-1)^3 \times 7 + (-1)^2 \times 9 + (-1)^1 \times 3 + 2 = 1 - 2 + 4 - 5 + 6 - 7 + 9 - 3 + 2 = 5 \pmod{11}. \text{ So remainder is } 5.$$

Proposition. \((\mathbb{Z}_n, \oplus, \oplus)\) is a unital commutative ring.

**Proof.** You have already seen why \((\mathbb{Z}_n, \oplus)\) is an abelian group.

So we will focus on other properties. All the properties can be easily deduced using congruence arithmetic:

$$a \oplus b \equiv a + b \pmod{n} \quad \text{and} \quad a \odot b \equiv ab \pmod{n}$$

as \(a \odot b\) is the remainder of \(a + b\) divided by \(n\), and \(a \oplus b\) is the remainder of \(ab\) divided by \(n\). So roughly using congruence arithmetic, we can “remove circles”.

\[(a \oplus b) \odot c \equiv (a \oplus b) c \pmod{n} \equiv (a + b) c \pmod{n} \quad \text{ (I)}\]
\[a \odot b \equiv a + b \pmod{n} \Rightarrow (a \oplus b) c \equiv (a + b) c \pmod{n} \]
Similarly \( a \odot c \equiv ac \pmod{n} \) \( \implies \)

\[ b \odot c \equiv bc \pmod{n} \]

\[ (a \odot c) + (b \odot c) \equiv ac + bc \pmod{n} \]

On the other hand \( (a \odot c) + (b \odot c) \equiv (a \odot c) \oplus (b \odot c) \pmod{n} \).

And so

\[ (a+b) \odot c \equiv (a \odot c) \oplus (b \odot c) \pmod{n} \] (II)

(II, III) imply \( (a \oplus b) \odot c \equiv (a \odot c) \oplus (b \odot c) \pmod{n} \)

And so \( (a \oplus b) \odot c \equiv (a \odot c) \oplus (b \odot c) \) as they are in \( \mathbb{Z}_0, 1, \ldots, n-1 \) and congruent modulo \( n \).

One can check other properties of a ring in a similar way.

Ex. Write addition and multiplication tables of \( \mathbb{Z}_4 \).

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

There is no 1 in this row, so 2 does not have a multiplicative inverse.
Ex. Find all the zeros of $x^2-x$ in $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

Solution. \[
\begin{array}{c|cc}
X & X-1 & X^2-X \\
\hline
0 & 4 & 0 \\
1 & 0 & 0 \\
2 & 1 & 2 \\
3 & 2 & 1 \\
4 & 3 & 2 \\
\end{array}
\hspace{1cm}
\begin{array}{c|cc}
X & X-1 & X^2-X \\
\hline
0 & 5 & 0 \\
1 & 6 & 0 \\
2 & 1 & 2 \\
3 & 2 & 0 \\
4 & 3 & 0 \\
5 & 4 & 2 \\
\end{array}
\]

Only two zeros 0 and 1. It has 4 zeros 0, 1, 3, 4. (This is NOT the same as zeros of polynomials in $\mathbb{C}$.)

As in group theory, we are interested in maps that preserve ring structure.

Def. Suppose $A$ and $B$ are rings. $f:A \rightarrow B$ is called a ring homomorphism if $f(a_1+a_2) = f(a_1) + f(a_2)$ and $f(a_1a_2) = f(a_1)f(a_2)$.

And a ring homomorphism $f:A \rightarrow B$ is called a ring isomorphism if $f$ is a bijection.