Let
\[ \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \]

We consider "funny" addition and multiplication in \( \mathbb{Z}_n \): we add and multiply as usual, but then divide the result by \( n \) and take the remainder.

**Examples:** \( \mathbb{Z}_6 \):

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
Note that 1 appears only in the first and fifth rows: 1 ⋅ 1 = 1, 5 ⋅ 5 = 1.

If a in \( \mathbb{Z}_n \) has the property that

\[ ab = 1 \]

for some b, we say that a is **invertible**.

So the invertible elements in \( \mathbb{Z}_6 \) are 1 and 5.

In general, a is invertible in \( \mathbb{Z}_n \) if \( ab = 1 + \text{multiple of } n \).
with respect to "usual" addition and multiplication. Thus

\[ ab = 1 + mn, \text{ or } \]

\[ b \cdot a + (-m) \cdot n = 1 \]

This means precisely that \( a \) and \( m \) are relatively prime. Let's emphasize it.

\[ a \text{ is invertible in } \mathbb{Z}_n \text{ if and only if } a \text{ and } m \text{ are relatively prime, i.e. } (a, n) = 1 \]

In previous example 1 and 5 are relatively prime to 6.

Let \( \mathbb{U}_n \) be the set of all invertible elements in \( \mathbb{Z}_n \), i.e. the set of all elements relatively prime to \( n \). Define

\[ \phi(n) = \text{number of elements in } \mathbb{U}_n \]

\( \phi \) is a very important function called the "Euler \( \phi \) function"
It is important how to compute it.

Here are the rules:

1. \( \phi(p) = p-1 \), if \( p \) is prime
2. \( \phi(ab) = \phi(a)\phi(b) \) if \( a, b \) are relatively prime.
3. \( \phi(p^n) = p^n - p^{n-1} \quad n \geq 2 \)

Example: \( \phi(328) = \phi(8\cdot41) = \phi(8)\cdot\phi(41) = \)

\[
\phi(8) = 4 \quad \text{rule 1}
\]

\[
\phi(41) = 40 \quad \text{rule 2}
\]

\[
\phi(328) = \phi(8\cdot41) = \phi(8)\cdot\phi(41) = 4\cdot40 = 160
\]

The Euler function \( \phi \) has important applications to cryptography.