3. \[ a \equiv b \pmod{n} \quad | \quad 3 \equiv 28 \pmod{5} \]
   \[ n \mid (a-b) \quad | \quad 5 \mid (3-28) \]

4. \[ \mathbb{Z}/n\mathbb{Z} = \{ a + n\mathbb{Z} : a \in \mathbb{Z} \} \]
   where \[ a+n\mathbb{Z} = \{ a+nk : k \in \mathbb{Z} \} \]

Those are the objects. Even better is to add "structure": operations.
We really use \[ \mathbb{Z}/n\mathbb{Z} \] as shorthand for \( (\mathbb{Z}/n\mathbb{Z}, +, \times) \) where \( a \) "+" and \( a \) "\times" is defined.

So, \[ \mathbb{Z}/3\mathbb{Z} = \{ 0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z} \} \]
noting that any \( a + 3\mathbb{Z} \) must be one of these.
and we can define operations directly with an addition and multiplication table

<table>
<thead>
<tr>
<th></th>
<th>0 + 3Z</th>
<th>1 + 3Z</th>
<th>2 + 5Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 + 3Z</td>
<td>0 + 3Z</td>
<td>1 + 3Z</td>
<td>2 + 5Z</td>
</tr>
<tr>
<td>1 + 3Z</td>
<td>1 + 3Z</td>
<td>2 + 3Z</td>
<td>0 + 3Z</td>
</tr>
<tr>
<td>2 + 3Z</td>
<td>2 + 3Z</td>
<td>1 + 3Z</td>
<td>1 + 3Z</td>
</tr>
</tbody>
</table>

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

5. A unit in \( \mathbb{Z}/n\mathbb{Z} \) is an element with a multiplicative inverse.

ex. In \( \mathbb{Z}/3\mathbb{Z} \), 2 + 3Z is its own multiplicative inverse.
That is, \((2+3z)(2+3z) = 1+3z\)

\[ \phi(n) = \sum_{1 \leq a \leq n \text{ such that } \gcd(a,n) = 1} a \]

**Example:**

\[ \phi(10) = \# \{1, 3, 7, 9\} = 4 \]

- \(\gcd(2, 10) > 1\)
- \(\gcd(4, 10) > 1\)
- \(\gcd(5, 10) > 1\)
- \(\gcd(6, 10) > 1\)
- \(\gcd(8, 10) > 1\)

**For every non-zero \(x\), prime \(p\)**

\[ x^{p-1} \equiv 1 \pmod{p} \]

**Example:**

When \(p = 5\)

- \(4^4 \equiv 1 \pmod{5}\)
- \(2^4 \equiv 16 \equiv 1 \pmod{5}\)
- \(3^4 \equiv 81 \equiv 1 \pmod{5}\)
- \(4^4 \equiv 256 \equiv 1 \pmod{5}\)

**Let \(p_1, p_2, \ldots, p_k\) be primes.**

Let \(p = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1\)

Note: \(p\) divided by any \(p_i\) has
remainder 1. That is, \( p \mid p \)

So \( p \) has a prime factor different from any of \( p_1, p_2, \ldots, p_k \)

That is, there must be another prime. This argument shows that there can't be a limit to the number of primes.

\[ \Rightarrow \]

Suppose \( a + n \in \mathbb{Z} \) a unit in \( \mathbb{Z}/n\mathbb{Z} \). So \( \exists b + n \mathbb{Z} \) such that \( (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \)

So \( ab \equiv 1 \pmod{n} \) and \( n \mid (ab - 1) \). So \( n \) has no non-trivial common factor with \( ab \) and thus not with \( a \). So \( \gcd(a, n) = 1 \)

\[ \Leftarrow \]

Suppose \( \gcd(a, n) = 1, 0 < a < n \)

Let \( U = \{a_i : \gcd(a_i, n) = 1, 0 \leq a_i < n\} \)

Note: \( a \in U \)

\[ 1 \in U \]

and the product of any pair
of elements of $U$ is in $U$.

Consider: $U' = \{a \cdot a_i : a_i \in U\}$

Suppose $a \cdot a_i \equiv a \cdot a_j \pmod{n}$

That is, $n \mid a(a_i - a_j)$

So, $n \mid (a_i - a_j)$

and $a_i \equiv a_j \pmod{n}$

So $U' \subseteq U$ and all elements are different. Thus $U = U'$

and $\exists a_i \in U$ with $a \cdot a_i = 1$

So $a + n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$

with inverse $a_i + n\mathbb{Z}$.

The example in the book is:

$11! + 2, 11! + 3, \ldots, 11! + 11$

Claim: $(a + n\mathbb{Z})^+ = \{b : a \equiv b \pmod{n}\}$

$(\subseteq)$ Let $a + nK \in a + n\mathbb{Z}$, $K \in \mathbb{Z}$
So \( a = a + nk \pmod{n} \)
So \( a + nk \in \{ b : a \equiv b \pmod{n} \} \)

(2) Let \( b \in \{ b : a \equiv b \pmod{n} \} \)
\( a \equiv b \pmod{n} \)
\( \Leftrightarrow n \mid (b-a) \)
\( \Leftrightarrow \exists k \in \mathbb{Z} \enspace nk = b-a \)
\( b = a + nk \)
\( \Rightarrow b \in a + n\mathbb{Z} \)

15.
\[ \text{gcd} (1, 10) = 1 \]
\[ \text{gcd} (2, 10) > 1 \]
\[ \text{gcd} (3, 10) = 1 \]
\[ \text{gcd} (4, 10) > 1 \]
\[ \text{gcd} (5, 10) > 1 \]
\[ \text{gcd} (6, 10) > 1 \]
\[ \text{gcd} (7, 10) = 1 \]
\[ \text{gcd} (8, 10) > 1 \]
\[ \text{gcd} (9, 10) = 1 \]
\[ \text{gcd} (10, 10) > 1 \]

So the units are:
1 + 10\( \mathbb{Z} \), 3 + 10\( \mathbb{Z} \), 7 + 10\( \mathbb{Z} \), 9 + 10\( \mathbb{Z} \)
16. If p is prime and 1 ≤ k < p then \( \gcd(k, p) = 1 \)

So \( 1 + pZ, 2 + pZ, \ldots, (p-1) + pZ \)

are all units in \( \mathbb{Z}/p\mathbb{Z} \)

17. If p is prime, every non-zero element of \( \mathbb{Z}/p\mathbb{Z} \) is a unit. So by definition \( \mathbb{Z}/p\mathbb{Z} \) is a field.

18. The order of \( 1 + 10Z \) is 1

\[ 1' \equiv 1 \pmod{10} \]

The order of \( 3 + 10Z \) is 4

\[ 3' \equiv 3, 3^2 \equiv 9, 3^3 \equiv 7, 3^4 \equiv 1 \pmod{10} \]

The order of \( 7 + 10Z \) is 4

\[ 7' \equiv 7, 7^2 \equiv 9, 7^3 \equiv 3, 7^4 \equiv 1 \pmod{10} \]

The order of \( 9 + 10Z \) is 2

\[ 9' \equiv 9, 9^2 \equiv 1 \pmod{10} \]
19. Suppose \( d | a, d | b, d | n \) and 
\( a \equiv b \pmod{n} \)
\( d \mid (a - b) \)
\( \exists k \in \mathbb{Z} \) such that 
\( n \mid (a - b) \)
\( d \mid n \) 
\( \exists k \in \mathbb{Z} \) such that 
\( n \mid (a - b) \)
\( d(a) = \exists a', d a' = a \quad a' = a/d \in \mathbb{Z} \)
\( d(b) = \exists b', d b' = b \quad b' = b/d \in \mathbb{Z} \)
\( d(n) = \exists n', d n' = n \quad n' = n/d \in \mathbb{Z} \)
so 
\( d n' k = d a' - d b' \)
so 
\( n' k = a' - b' \)
so 
\( a' \equiv b' \pmod{n'} \)
or 
\( \frac{a}{d} = \frac{b}{d} \pmod{\frac{n}{d}} \)
\( \checkmark \)

20. Suppose \( a_r, \ldots, a_n \) is a complete set of residues mod \( n \) and \( a \) is a unit \( \pmod{n} \).
Consider: \( a \cdot a_r, a \cdot a_2, \ldots, a \cdot a_n \) (mod \( n \))
Suppose \( a \cdot a_i = a \cdot a_j \) (mod \( n \))
so \( n \mid a \cdot a_j \)
\[
\iff n \mid a (a_i - a_j)
\]

Since \( \gcd(n, a) = 1 \) we must have \( n \mid (a_i - a_j) \)

That is, \( a_i \equiv a_j \pmod{n} \)

and we then conclude all of \( a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_n \pmod{n} \)
are different.