Theorem (Fundamental theorem of arithmetic)

Let $n \in \mathbb{N}$ with $n \geq 2$. Then

(i) $n = p_1 \ldots p_r$, where each $p_i$ is prime, and

(ii) any two such expressions for $n$ differ only in the order of writing.

Proof.

On board

Corollary

Let $n \in \mathbb{N}$ with $n \geq 2$. Then we may uniquely write

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r},$$

where $p_1 < p_2 < \cdots < p_r$ are primes and each $\alpha_j \in \mathbb{N}$. 
Fermat’s little theorem

Example:
Let $p = 5$ and $a \in \{1, 2, 3, 4\}$.

Notice

\[
\begin{array}{c|cccc}
  a & 1 & 2 & 3 & 4 \\
  \hline 
  a^5 & 1 & 32 & 243 & 1024 \\
  a^5 - a & 0 & 30 & 240 & 1020 \\
\end{array}
\]

In each case $5 \mid a^5 - a$.

This is explained by:

**Theorem (Fermat’s little theorem)**

Let $p \in \mathbb{N}$ be prime, and let $a \in \mathbb{N}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

**Proof.**

*On board*
An alternative (equivalent) formulation is:

**Theorem (Fermat’s little theorem)**

Let $p \in \mathbb{N}$ be prime, and let $a \in \mathbb{N}$. Then $a^p \equiv a \mod p$.

**Examples:**

*On board*
Section 11: Binary operations

Let $S$ be a set.

A *binary operation* $\ast$ on $S$ is a function

$$\ast : S \times S \to S.$$  

For convenience we write $a \ast b$ instead of $\ast(a, b)$.

**Examples:**

(i) Let $S = \mathbb{R}$ and $\ast$ be $+$. For $a, b \in \mathbb{R}$, $a \ast b = a + b$, addition. This is a binary operation.

(ii) Let $S = \mathbb{Z}$ and $\ast$ be $\times$. For $a, b \in \mathbb{Z}$, $a \ast b = ab$, multiplication. This is a binary operation.

(iii) Let $S = \mathbb{Z}$. For $a, b \in \mathbb{Z}$, define $a \ast b = \max\{a, b\}$, the largest of $a$ and $b$. This is a binary operation.

(iv) Let $S = \mathbb{Q}$ and define $\ast$ by $a \ast b = a$. This is a binary operation.
(v) Let $S = \mathbb{Z}$ and $a \ast b = \frac{a}{b}$.
This is not a binary operation, as it’s not defined when $b = 0$, and also $\frac{a}{b}$ need not be in $\mathbb{Z}$.

(vi) Let $S = \{f : \mathbb{Z} \to \mathbb{Z}\}$, with $f \ast g = f \circ g$, composition of functions.
This is a binary operation.

(vii) Let $S = \mathbb{N}$, with $\ast$ defined by $a \ast b = a^b$ (e.g., $2 \ast 3 = 2^3 = 8$). This is a binary operation.
For small sets, we may record a binary operation using a table, called the *multiplication table* (whether or not the binary operation is multiplication).

For example, let $S = \{\alpha, \beta, \gamma\}$. Define a binary operation $\ast$ as follows:

<table>
<thead>
<tr>
<th>$\ast$</th>
<th>$\alpha$</th>
<th>$\beta$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\gamma$</td>
<td>$\beta$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>$\alpha$</td>
<td>$\beta$</td>
<td>$\beta$</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>$\beta$</td>
<td>$\alpha$</td>
<td>$\gamma$</td>
</tr>
</tbody>
</table>

where we take the row first and then the column.

So, for example, $\alpha \ast \beta = \gamma$, $\beta \ast \alpha = \alpha$, etc.

In general, if $S = \{a_1, \ldots, a_n\}$, then the entry in the row labeled by $a_j$ and column labeled by $a_i$ is $a_j \ast a_i$.

**Example:** $S = \mathbb{Z}_4$, $\ast = \oplus$.

_On board_