**Theorem (7.7.4)**
$\bar{c} \in \mathbf{Z}_n$ is invertible if and only if $\gcd(c,n) = 1$.

**Corollary (7.7.6)**
If $p$ is prime, then every non-zero element of $\mathbf{Z}_p$ is invertible.

This result allows us to define arithmetic operations on the set of integers modulo $n$ as follows:

$\overline{a} +_n \overline{b} = \overline{a+b}$ $\qquad\qquad$ $\overline{a} \cdot_n \overline{b} = \overline{ab}$

**Theorem (7.6.7, 7.7.1)**
1. $+_n$ and $\cdot_n$ are binary operations on $\mathbf{Z}_n$.

2. $+_n$ and $\cdot_n$ are associative and commutative.

3. The distributive law holds. That is,
$\forall \overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}_n,\ (\overline{a} +_n \overline{b}) \cdot_n \overline{c} = \overline{a} \cdot_n \overline{c} +_n \overline{b} \cdot_n \overline{c}$

4. $\overline{0}, \overline{1}$ act as identity elements under $+_n$ and $\cdot_n$ respectively.

5. $+_n$ -inverses exist. That is,
$\forall \overline{a} \in \mathbf{Z}_n,\ \exists \overline{b} \in \mathbf{Z}_n,\ \overline{a} +_n \overline{b} = \overline{0}$

6. $+_n$ -cancellation holds. That is,
$\forall \overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}_n,\ \overline{a} +_n \overline{b} = \overline{a} +_n \overline{c} \Rightarrow \overline{b} = \overline{c}$

**Example**
$\cdot_n$ -inverse and $\cdot_n$ -cancellation do not always work.

## Congruences (¶7.6)

Let $n \in \mathbf{N}$. Define a relation ~ on $\mathbf{Z}$ by
$a \sim b \Leftrightarrow n \mid a - b$

$\sim$ is an equivalence relation called "congruence modulo *n*."

We write $a \equiv b \bmod n$ to mean $n \mid a - b$.

**Examples**

**Note (7.6.4)**: $a \equiv b \bmod n$ if and only if *a,b* leave the same remainder when divided by *n*.

## Congruence classes

$\bar{a} = \{x \in \mathbf{Z} \; : \; a \equiv x \bmod n\}$

$\bar{0}, \bar{1}, \cdots, \overline{n-1}$ are non-overlapping subsets of $\mathbf{Z}$ that cover **Z**.

$\mathbf{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ is called the set of *integers modulo n.*

**Theorem (7.6.6)**
$\forall n \in \mathbf{N}, \forall a, b, c \in \mathbf{Z}$, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then

1. $a + c \equiv b + d \bmod n$
2. $ac \equiv bd \bmod n$

**Corollaries**

1. Every integer other than 0, $\pm 1$ is uniquely expressible in the form $a = up_1^{e_1} \cdots p_n^{e_n}$ with $u = \pm 1$, $p_i$ distinct primes, and $e_i \in \mathbf{N}$.

2. If $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$ with $p_i$ distinct primes, and $e_i, f_i \geq 0$, then $a \mid b$ if and only if $e_i \leq f_i$ for all $i$.

3. If $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$ with $p_i$ distinct primes, and $e_i, f_i \geq 0$, then

$$\gcd(a,b) = \prod_{i=1}^{n} p_i^{g_i} \quad \text{where} \quad g_i = \min\{e_i, f_i\}$$

4. $\forall a,b \in \mathbf{N}$, $a,b$ have a unique least common multiple, and it is given by $m = \dfrac{ab}{\gcd(a,b)}$.

5. $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.

# Fundamental Theorem of Arithmetic (¶7.5)

**Preliminaries**:

1. Every $n \in \mathbf{N}$ is a prime or a product of primes.

2. $\forall a,b,c \in \mathbf{Z}$ if $a \mid bc$ and $\gcd(a,b)=1$ then $a \mid c$.

3. If $p$ is prime, then $\forall a,b \in \mathbf{Z}$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

3'. If $p$ is prime, then $\forall a_1,\cdots,a_n \in \mathbf{Z}$, if $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some $i$.

**Theorem (FTA)**

Every integer $>1$ is uniquely (up to order of factors) expressible as a product of primes.

**Proof**:

Existence:(1. above)

Uniqueness: (proof by induction) Let $P_n$ be the statement, "For any integer that can be written as a product of $n$ primes, the factorization is unique up to order of factors."