$n \geq 2$ integer define on $\mathbb{Z}$ the equivalance relation

$$x \equiv y \mod n \iff n \mid x - y$$

$$x \overset{n}{\equiv} y$$

The $\bar{x} = \{x + kn \mid k \in \mathbb{Z}\}$

Denote $\mathbb{Z}_n = \{\bar{x} \mid x \in \mathbb{Z}\} = \mathbb{Z} / \overset{n}{\equiv}$

Lemma: For n fixed: $x \equiv y \mod n \iff$ x and y have the same reminders when divided by n

Proof: "⇒" Assume $n \mid x-y$

We write $x = q \cdot n + r_1$

$y = q' \cdot n + r_2$ —

$x - y = n(q_1 - q_2) + (r_1 - r_2)$ } ⇒

$0 \le r_1, r_2 < n$ $\quad n \mid x-y$ }

⇒ $|r_1 - r_2| < n$

$n \mid r_1 - r_2$ } ⇒ $|r_1 - r_2| = 0 \Rightarrow r_1 = r_2$

"⇐" If $r_1 = r_2$ when dividing x and y by n ⇒ $x - y = n(q_1 - q_2) \Rightarrow n \mid x-y \Rightarrow$

$\Rightarrow x \equiv y \mod n$

Corollary: $\{0, 1, 2, \dots, n-1\}$ is a system of representatives for $\equiv$

$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}$

$\hat{0}$ in $\mathbb{Z}_2 = \{2k \mid k \in \mathbb{Z}\}$

$\hat{0}$ in $\mathbb{Z}_5 = \{5k \mid k \in \mathbb{Z}\}$

Lemma: $n \geq 2$ fixed integers. Let $x_1, x_2, y_1, y_2 \in \mathbb{Z}$

1) If $\begin{matrix} x_1 \equiv x_2 \bmod n \\ y_1 = y_2 \bmod n \end{matrix}$, then $\begin{cases} x_1 + y_1 \equiv x_2 + y_2 \bmod n \\ x_1 \cdot y_1 = x_2 \cdot y_2 \bmod n \end{cases}$

2) In particular, if $x_1 \equiv x_2 \bmod n \Rightarrow$

$$\Rightarrow \begin{cases} x_1 + a = x_2 + a \bmod n \\ x_1 \cdot a = x_2 \cdot a \bmod n \end{cases}$$

Proof 1) $n \mid x_1 - x_2 \Rightarrow x_1 - x_2 = n \cdot k_1$ $\quad k_1, k_2 \in \mathbb{Z}$
$n \mid y_1 - y_2 \Rightarrow y_1 - y_2 = n \cdot k_2$

$\oplus$

$$(x_1 - x_2) + (y_1 - y_2) = n(k_1 + k_2)$$

$$(x_1 + y_1) - (x_2 + y_2) = n(k_1 + k_2)$$

$\Rightarrow x_1 + y_1 \equiv x_2 + y_2 \bmod n$ ✓

$$x_1 \cdot y_1 - x_2 \cdot y_2 = x_1(y_1 - y_2) + x_1 y_2 - x_2 y_2$$

$$= x_1(y_1 - y_2) + y_2(x_1 - x_2)$$

$$= x_1 \cdot n \cdot k_2 + y_2 \cdot n \cdot k_1$$

$$\Rightarrow n \mid x_1 \cdot y_1 - x_2 \cdot y_2 \Rightarrow$$

$$\Rightarrow x_1 \cdot y_1 \equiv x_2 y_2 \mod n$$

On $\mathbb{Z}_n$ define „+": $\hat{x} + \hat{y} := \widehat{x+y}$

„·": $\hat{x} \cdot \hat{y} := \widehat{x \cdot y}$

These operations are well defined:
they do not depend on the representatives chosen in the class

If $\hat{x_1} = \hat{x_2}$ and $\hat{y_1} = \hat{y_2} \Rightarrow \begin{cases} \widehat{x_1 + y_1} = \widehat{x_2 + y_2} \\ \widehat{x_1 \cdot y_1} = \widehat{x_2 \cdot y_2} \end{cases}$

$\hat{x_1} = \hat{x_2} \Leftrightarrow n \mid x_1 - x_2$

$\hat{y_1} = \hat{y_2} \Leftrightarrow n \mid y_1 - y_2$

Proved in the Lemma before

Proposition: For $n \geq 2$: $(\mathbb{Z}_n, +, \cdot)$ is a comutative ring

Prof: Check $(\mathbb{Z}_n, +)$ is an abelian group

1) „+" is associative on $\mathbb{Z}_n$

$\forall \hat{x}, \hat{y}, \hat{z} \in \mathbb{Z}_n : (\hat{x} + \hat{y}) + \hat{z} = \hat{x} + (\hat{y} + \hat{z})$

$(\hat{x+y}) + \hat{z} \overset{''}{=} \hat{x} + (\hat{y+z})$

$(x+y) + z = x + (y+z)$

2) $\hat{0}$ is the neutral element for „+"

$\forall \hat{x} \in \mathbb{Z}_n \quad \hat{x} + \hat{0} = \hat{0} + \hat{x} = \hat{x}$

$\hat{x+0} = \hat{0+x} = \hat{x}$

3) $\forall x \in \mathbb{Z}_n$ it has a symmetric: $\hat{-x}$

$\hat{x} + \hat{-x} = \hat{-x} + \hat{x} = \hat{0}$

$\hat{x + (-x)} = \hat{0}$

4) $\hat{x} + \hat{y} = \hat{y} + \hat{x}$ True

$\hat{x+y} = \hat{y+x}$

5) „$\cdot$" is associative on $\mathbb{Z}_n$:

$\forall \hat{x}, \hat{y}, \hat{z} \in \mathbb{Z}_n \quad (\hat{x} \cdot \hat{y}) \cdot \hat{z} = \hat{x} \cdot (\hat{y} \cdot \hat{z})$

6) $\hat{1}$ is the neutral element for „$\cdot$"

$\forall \hat{x} \in \mathbb{Z}_n \quad \hat{x} \cdot \hat{1} = \hat{1} \cdot \hat{x} = \hat{x}$

7) „$\cdot$" is commutative: $\hat{x} \cdot \hat{y} = \hat{y} \cdot \hat{x}, \forall \hat{x}, \hat{y} \in \mathbb{Z}_n$

$\hat{x \cdot y} = \hat{y \cdot x}$

8) „$\cdot$" is distributive w.r.t. „$+$"

$\hat{x} \cdot (\hat{y} + \hat{z}) = \hat{x} \cdot \hat{y} + \hat{y} \cdot \hat{z}$

$(\hat{y} + \hat{z}) \cdot \hat{x} = \hat{y} \cdot \hat{x} + \hat{z} \cdot \hat{x}$

Denote $U(\mathbb{Z}_n) = \{\hat{x} \in \mathbb{Z}_n \mid \hat{x}$ is invertable $\}$

$\exists \hat{y} \in \mathbb{Z}_n : \hat{x} \cdot \hat{y} = \hat{1}$

a.k.a the units of $\mathbb{Z}_n$

$\hat{x} \cdot \hat{y} = \hat{1} \Leftrightarrow \hat{x \cdot y} = \hat{1} \Leftrightarrow xy = 1 \bmod n$

$\Leftrightarrow \exists k \in \mathbb{Z} \quad 1 - xy = k \cdot n$

$U(\mathbb{Z}_n) = \{\hat{x} \in \mathbb{Z}_n \mid \exists y, k \in \mathbb{Z}$ s.t. $x \cdot y + k \cdot n = 1\}$

$U(\mathbb{Z}_n) = \{\hat{x} \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$

$|U(\mathbb{Z}_n)| = |\{x \in \mathbb{Z} \mid 0 \le x < n \quad \gcd(x, n) = 1\}|$

$= \varphi(n) \rightarrow$ Euler's function

Fact: if $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ prime decomposition

$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right)$

Example:

$U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$

$\varphi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2$

$6 = 2 \cdot 3$

$p_1 \quad p_2$

Prop: $\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is prime

field i.e. any non-zero element is invertable