Recall: Fix \( n \in \mathbb{N} \). For \( a, b \in \mathbb{Z} \),

\[ a = b \mod n \iff n \mid (b - a). \]

\([a] = \{ b \in \mathbb{Z} \mid b = a \mod n \} \]

\( \mathbb{Z}_n = \{ [a] \mid a \in \mathbb{Z}, [a] = [0], \ldots, [n-1] \} = \{ [0], [1], [2], \ldots \} = \ldots \)

\( a = a' \) and \( b = b' \mod n \Rightarrow a + b = a' + b' \) and \( ab = a'b' \mod n \)

**Can define** \([a] + [b] = [a + b] \) and \([a] \cdot [b] = [ab] \).

- Independent of representatives \( a \) and \( b \) of congruence class by \( \equiv \).

- and \( \cdot \) are **commutative** and **associative**, **distributive law**

- \([0]\) is an identity for + (additive identity)

- \([1]\) is a multiplicative identity (multiplicative identity)

\((\mathbb{Z}_n, +)\) is a group [[What does this mean again?]]

\((\mathbb{Z}_n, \cdot)\) a group? No! \([0] \) must be identity, but \([0]\) has no inverse.

**Proposition 1.9.** For \( n \in \mathbb{Z} \), \([a] \in \mathbb{Z}_n\) has a multiplicative inverse if \( \gcd(a, n) = 1 \)

**Proof:** Suppose \( \exists [b] \in \mathbb{Z}_n \) s.t. \([a] [b] = [1] \). That is \( ab = 1 \mod n \).

\( \Rightarrow n \mid (1 - ab) \Rightarrow \exists t \in \mathbb{Z} \) s.t. \( tn = 1 - ab \Rightarrow 1 = tn + ab \), so \( \gcd(a, n) = 1 \).

Conversely, if \( \gcd(a, n) = 1 \) then \( \exists b, t \in \mathbb{Z} \) s.t. \( ba + tn = 1 \Rightarrow tn = 1 - ba \)

\( \Rightarrow n \mid (1 - ba) \Rightarrow ba = 1 \mod n \Rightarrow [b][a] = [1] \quad \square \)

Let \( \mathbb{Z}_n^\times = \{ [a] \in \mathbb{Z}_n \mid \gcd(a, n) = 1 \} \). Then \( \mathbb{Z}_n^\times = \{ [a] \in \mathbb{Z}_n \mid [a] \) has a multiplicative inverse \}

Note: \([a] \) in \( a \) is a mult inverse for \([a] \in \mathbb{Z}_n^\times \).
\[ \mathbb{E}_x : \mathbb{Z}_7^* = \{ [1], [5], [7], [-1] \} \]
\[ \mathbb{Z}_7^* = \{ [1], [5], [3], [-4], [2], [6] \} \]

**Proposition** \((\mathbb{Z}_n^*, \cdot)\) is a group

**Proof.** is an operation on \(\mathbb{Z}_n^*\). [What?]

\[ [a], [b] \in \mathbb{Z}_n^* \Rightarrow ([a][b]) \cdot ([a]^{-1} [a]^{-1}) = [a][b][a]^{-1} [a]^{-1} = [1][1] = [1] \]

associative, \( [1] \) identity, inverse \( \exists aT \in \mathbb{Z}_n^* ? \)

\[ [a]^{-1} \cdot [a] = [1] \Rightarrow ([a]^{-1})^{-1} = [a] \text{ and } [a] \in \mathbb{Z}_n^* \]

**Zero divisors** \( [a] \cdot [b] = [0] \Rightarrow [a] \neq [0], [b] \neq [0] \Rightarrow \exists [a][b] = [1] \).

**Exercise:** show \( [a] \in \mathbb{Z}_n^* \) is a zero divisor iff \( [a] \neq \) and \( [a] \in \mathbb{Z}_n^* \).

How many elements in \( \mathbb{Z}_n^* \)? Define Euler \( \varphi \)-function by

\[ \varphi(n) = |\mathbb{Z}_n^*| \]

- \( p \) a prime, \( \varphi(p) = p-1 \): every number \( 1, 2, \ldots, p-1 \) is rel. prime to \( p \).
- \( k \geq 2 \), \( \varphi(p^k) = ? \): which number in \( \{ 1, 2, \ldots, p^k \} \) are rel. prime to \( p^k \)?

all those not multiples of \( p \): \( \{ p, 2p, 3p, \ldots, p^2, \ldots, p^k \} \) all with \( \varphi(p) = p-1 \).

**Then**, so

\[ \varphi(p^k) = p^{k-1} (p-1) \]

--- See §1.9 ---
Proposition (Ca 1.9.19): \( \gcd(m,n)=1 \) then \( \varphi(mn) = \varphi(m) \varphi(n) \).

Using prime factorization, this gives \( \varphi(n) \) \( \forall n \in \mathbb{Z}^+ \): \( n = p_1^{k_1} \cdots p_r^{k_r} \)

\[ \varphi(n) = \varphi(p_1^{k_1} \cdots p_r^{k_r}) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r}) = p_1^{k_1} \left( 1 - \frac{1}{p_1} \right) \cdots p_r^{k_r} \left( 1 - \frac{1}{p_r} \right) \]

\[ = p_1^{k_1} \left( 1 - \frac{1}{p_1} \right) p_2^{k_2} \left( 1 - \frac{1}{p_2} \right) \cdots p_r^{k_r} \left( 1 - \frac{1}{p_r} \right) \]

Proposition follows from

Proposition 1.7.9 (Chinese remainder theorem): \( \gcd(a,b)=1 \), \( a,b \in \mathbb{Z}^+ \).

Then \( \exists x \in \mathbb{Z} \) s.t.

\[ x \equiv a \mod{a} \quad \text{and} \quad x \equiv b \mod{b} \]

Moreover, \( x \) is unique modulo \( ab \).

That \( x \equiv y \mod{ab} \), then \( x \equiv y \mod{a} \) and \( x \equiv y \mod{b} \), since \( ab | x - y \implies a | x - y \) and \( b | x - y \).

Proof of CRT: \( \exists a, b \in \mathbb{Z} \) s.t. \( a + bt = 1 \) s.t.

\[ x_1 = 1 - ta = tb \quad \text{and} \quad x_2 = 1 - tb = ta \]

\[ \implies x \equiv 1 \mod{a} \quad \text{and} \quad x \equiv 0 \mod{b} \]
\[ x \equiv 0 \mod{a} \quad \text{and} \quad x \equiv 1 \mod{b} \]

\[ \text{Set} \ x = ax_1 + bx_2 \equiv \begin{cases} a \mod{a} \\ b \mod{b} \end{cases} \]
Uniqueness: Two solns \(x, x'\), then
\[ a \mid x - x' \quad \text{and} \quad b \mid x - x' \quad \text{exercise since} \ \gcd(a, b) = 1 \]
\[ \quad \Rightarrow ab \mid x - x' \quad \Rightarrow x - x' \mod ab \square \]

Proof: that \( \varphi(mn) = \varphi(m) \varphi(n) \) if \( \gcd(m, n) = 1 \):

Can define \( \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^* \)
\[ [a]_{mn} \mapsto ([a]_m, [a]_n) \]

By CRT, this is a bijection \( \square \).