L7: Chinese Remainder Theorem
Solve the following simultaneous congruence equations:

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 2 \pmod{7} \]
Solve: \( x \equiv 2 \pmod{3} \quad x \equiv 3 \pmod{5} \quad x \equiv 2 \pmod{7} \)

3, 5, 7 pairwise prime: \( \gcd(3, 5) = \gcd(5, 7) = \gcd(3, 7) = 1 \)

First, solve the following:

\[
\begin{align*}
    d_3 & \equiv 1 \pmod{3} & d_5 & \equiv 0 \pmod{3} & d_7 & \equiv 0 \pmod{3} \\
    d_3 & \equiv 0 \pmod{5} & d_5 & \equiv 1 \pmod{5} & d_7 & \equiv 0 \pmod{5} \\
    d_3 & \equiv 0 \pmod{7} & d_5 & \equiv 0 \pmod{7} & d_7 & \equiv 1 \pmod{7} \\
    d_3 & \equiv 70 \pmod{105} & d_5 & \equiv 21 \pmod{105} & d_7 & \equiv 15 \pmod{105}
\end{align*}
\]

\[
\begin{align*}
    35 \cdot 2 & \equiv 1 \pmod{3} & 21 \cdot 1 & \equiv 1 \pmod{5} & 15 \cdot 1 & \equiv 1 \pmod{7}
\end{align*}
\]

Solution: \( x \equiv 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 \pmod{105} \)

\[
\begin{align*}
    & \equiv 35 + 63 + 30 \pmod{105} \\
    & \equiv 128 \pmod{105} \\
    & \equiv 23 \pmod{105}
\end{align*}
\]
Thm: [Sun Zi, Qin Jiushao 1247] Let moduli $m_1, \ldots, m_k$ be pairwise prime, let $P = m_1 \cdot m_2 \cdots m_k$. For all $a_1 \ldots a_k$, there exists a unique solution \( (\mod P) \) to the simultaneous equations

\[
x \equiv a_1 \pmod{m_1} \quad x \equiv a_2 \pmod{m_2} \quad \cdots \quad x \equiv a_k \pmod{m_k}.
\]

**proof:** Let $q_i = P/m_i = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_k$. $\gcd(q_i, m_i) = 1$. Using Euclid’s Algorithm, compute $(q_i)^{-1}_{m_i}$.

Let $d_i = q_i \cdot (q_i)^{-1}_{m_i}$ \quad $d_i \equiv 1 \pmod{m_i}$ \quad $d_i \equiv 0 \pmod{m_j}$, $j \neq i$

\[
b = d_1 \cdot a_1 + d_2 \cdot a_2 + \cdots + d_m \cdot a_m \quad b \equiv a_i \pmod{m_i}.
\]

$b$ is unique by counting: $P = m_1 \cdot m_2 \cdots m_k$ possible choices for $a_1, \ldots, a_k$, corresponding to exactly all the $P$ elements of $\mathbb{Z}_P$. \qed
Solve: \( x \equiv a_1 \pmod{3} \quad x \equiv a_2 \pmod{5} \quad x \equiv a_3 \pmod{7} \)

First, solve the following:

\[
\begin{align*}
    d_3 & \equiv 1 \pmod{3} & d_5 & \equiv 0 \pmod{3} & d_7 & \equiv 0 \pmod{3} \\
    d_3 & \equiv 0 \pmod{5} & d_5 & \equiv 1 \pmod{5} & d_7 & \equiv 0 \pmod{5} \\
    d_3 & \equiv 0 \pmod{7} & d_5 & \equiv 0 \pmod{7} & d_7 & \equiv 1 \pmod{7} \\
    d_3 & \equiv 70 \pmod{105} & d_5 & \equiv 21 \pmod{105} & d_7 & \equiv 15 \pmod{105} \\
    35 \cdot 2 & \equiv 1 \pmod{3} & 21 \cdot 1 & \equiv 1 \pmod{5} & 15 \cdot 1 & \equiv 1 \pmod{7}
\end{align*}
\]

Example: \( a_1 = 1, \quad a_2 = 2, \quad a_3 = 3 \)

Solution: \( x \equiv d_3 \cdot a_1 + d_5 \cdot a_2 + d_7 \cdot a_3 \pmod{105} \)

Solution: \( x \equiv 70 \cdot 1 + 21 \cdot 2 + 15 \cdot 3 \pmod{105} \)

\[
\begin{align*}
    &\equiv 70 + 42 + 45 \pmod{105} \\
    &\equiv 157 \pmod{105} \\
    &\equiv 52 \pmod{105}
\end{align*}
\]
\( \forall a, m > 1 \ (a \text{ has mult. inverse mod } m \text{ iff } \gcd(a, m) = 1) \)

<table>
<thead>
<tr>
<th>( \times \mod 6 )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
∀a, m > 1 (a has mult. inverse mod m iff gcd(a, m) = 1)

**Def:** \(\mathbb{Z}_m^* = \{a \mid 0 < a < m \land \text{gcd}(a, m) = 1\}\)

This is the **multiplicative group** mod m.

\(\mathbb{Z}_m^*\) is the set of positive integers less than m that are relatively prime to m, with multiplication mod m.

\[
\begin{array}{c|cccc}
\mathbb{Z}_6^* & 1 & 5 \\
1 & 1 & 5 \\
5 & 5 & 1 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\mathbb{Z}_5^* & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 \\
2 & 2 & 4 & 1 & 3 \\
3 & 3 & 1 & 4 & 2 \\
4 & 4 & 3 & 2 & 1 \\
\end{array}
\]
\[ \mathbb{Z}_m^* = \{ a \mid 0 < a < m \land \gcd(a, m) = 1 \} \]

\( \mathbb{Z}_m^* \) is the **multiplicative group mod m**.

A **group** is a set \( G \), with a binary operation \( \star \), s.t.

- **G is associative**: \( \forall abc \in G \ (a \star (b \star c) = (a \star b) \star c) \)
- **G has an identity element**, \( 1 \), \( \forall a \in G \ (a \star 1 = 1 \star a = a) \)
- **G has inverses**: \( \forall a \in G \ \exists a^{-1} \in G (a \star a^{-1} = a^{-1} \star a = 1) \)

\[
\begin{array}{c|cc}
\mathbb{Z}_6^* & 1 & 5 \\
\hline
1 & 1 & 5 \\
5 & 5 & 1 \\
\end{array}
\]

\[
\begin{array}{c|cc}
\mathbb{Z}_3^* & 1 & 2 \\
\hline
1 & 1 & 2 \\
2 & 2 & 1 \\
\end{array}
\]

\( \mathbb{Z}_6^* \) and \( \mathbb{Z}_3^* \) are **isomorphic** \( (\mathbb{Z}_6^* \cong \mathbb{Z}_3^*) \). This means they are **identical**: only the names of their elements are changed.
Cyclic Groups

**Def:** An $n$-element group, $G$, is **cyclic** iff it has an element $g \in G$ called a **generator** s.t. $G = \langle g \rangle = \{g, g^2, g^3, \ldots, g^n = 1\}$.

**Fact:** For all primes, $p$, $\mathbb{Z}_p^*$ is cyclic.

**iClicker:** What are the generators of $\mathbb{Z}_3^*$?
- **A:** $\{1\}$
- **B:** $\{2\}$
- **C:** $\{1, 2\}$

**iClicker:** What are the generators of $\mathbb{Z}_5^*$?
- **A:** $\{1, 4\}$
- **B:** $\{1, 2\}$
- **C:** $\{2, 3\}$
- **D:** $\{3, 4\}$
**Def:** If \( g \) is a generator of the group \( \mathbb{Z}_m^* \), and \( a \in \mathbb{Z}_m^* \), then \( \log_g a \pmod{m} = e \) iff \( g^e \equiv a \pmod{m} \).

<table>
<thead>
<tr>
<th>( \mathbb{Z}_3^* )</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

\[
\log_2(1) \pmod{3} = 2 \\
\log_2(2) \pmod{3} = 1
\]

**iClicker:** What is \( \log_3 2 \pmod{5} \) ?

- A: 1, B: 2, C: 3, D: 4
**Thm:** [Fermat, 1640] Let \( p \) be prime, and \( a \in \mathbb{Z}_p^* \). Then:

\[
a^{p-1} \equiv 1 \pmod{p}.
\]

**proof:** Let \( f_a : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^* \) be given by \( f_a(x) = (a \cdot x) \% p \)

**Claim:** \( f_a \) is 1:1 and onto.

**proof:** Suppose that for some \( b, c \in \mathbb{Z}_p^* \),

\[
\begin{align*}
f_a(b) &= f_a(c) \\
a \cdot b &\equiv a \cdot c \pmod{p} \\
a_p^{-1} \cdot a \cdot b &\equiv a_p^{-1} \cdot a \cdot c \pmod{p} \\
b &\equiv c \pmod{p} \\
b &= c
\end{align*}
\]

Thus, \( f_a \) is 1:1.
Thm: For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

Lemma: For a finite set $S$, if $f : S \xrightarrow{1:1} S$, then $f : S \xrightarrow{1:1\text{ onto}} S$.

Let $S = \{a_1, a_2, \ldots, a_n\}$

Since $f$ is 1:1, $f(a_1), f(a_2), \ldots, f(a_n)$ are distinct elements of $S$.

Thus, $S = \{f(a_1), f(a_2), \ldots, f(a_n)\}$. \hfill $\square$

Thus, $f_a(x) = (a \cdot x)$ is 1:1 and onto. \hfill $\square$

We say that $f_a : \mathbb{Z}_p^* \xrightarrow{1:1\text{ onto}} \mathbb{Z}_p^*$ is a permutation of $\mathbb{Z}_p^*$. 

L7: Chinese Remainder Theorem

CS250: Discrete Math for Computer Science
Thm: For \( p \) prime, \( a \in \mathbb{Z}_p^* \), \( a^{p-1} \equiv 1 \pmod{p} \)

**proof:** \( f_a : \mathbb{Z}_p^* \xrightarrow{1:1 \text{ onto}} \mathbb{Z}_p^*; \ f_a(x) = (a \cdot x) \)

\[
\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}
\]

\[
\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}
\]

\[
\prod_{i \in \mathbb{Z}_p^*} i \equiv \prod_{i \in \mathbb{Z}_p^*} a \cdot i \pmod{p}
\]

\[
\prod_{i \in \mathbb{Z}_p^*} i \equiv a^{p-1} \prod_{i \in \mathbb{Z}_p^*} i \pmod{p}
\]

\[
1 \equiv a^{p-1} \pmod{p} \quad \square
\]