Solving linear congruences \( ax \equiv b \mod n \):

1) \( ax \equiv b \mod n \) has an inverse if \( \gcd(a, n) = 1 \)
\[ ax + ny = \gcd(a, n) = 1 \] by Bezout's Identity
\[ \Rightarrow ax = 1 + n(-y) \Rightarrow ax \equiv 1 \mod n \]
(Recall the modular **multiplicative inverse** of 
\[ a \in \mathbb{Z} \text{ is } x \in \mathbb{Z} \text{ s.t. } ax \equiv 1 \mod n \]
\[ \Rightarrow x = a^{-1} \] can be found using the Extended Euclidean Algorithm)

2) \( ax \equiv b \mod n \) has a solution if \( \gcd(a, n) \mid b \)

3) If \( ax \equiv b \mod n \) has a solution, i.e. \( \gcd(a, n) \mid b \),
then there are \( \gcd(a, n) \) solutions separated by \( \frac{n}{\gcd(a, n)} \)

4) \( ca \equiv cb \mod n \) \( \iff \) \( a \equiv b \mod \frac{n}{\gcd(c, n)} \)
(We can simplify and cancel a factor of \( c \)
but we do not end up in the same modular space.)
Ex: Modular Inverses

Find \( 34^{-1} \mod 143 \) \( \iff 34x \equiv 1 \mod 143 \)

Apply Bezout's Identity: \( 34x + 143y = \gcd(34, 143) \)

(i) \( 143 = 4 \times 34 + 7 \Rightarrow 7 = 143 - 4 \times 34 \)

(ii) \( 34 = 4 \times 7 + 6 \Rightarrow 6 = 34 - 4 \times 7 \)

(iii) \( 7 = 1 \times 6 + 1 \Rightarrow 1 = 7 - 1 \times 6 \)

\( \Rightarrow \gcd(34, 143) = 1 \Rightarrow \exists x \text{ s.t. } ax \equiv 1 \mod 143 \)

where \( x = a^{-1} \)

Step 1: Find \( x \), the inverse and the Bezout Coefficient:

\[
6 = 34 - 4 \times (143 - 4 \times 34)
\]

\[
= 17 \times 34 - 4 \times 143
\]

\[
1 = 143 - 4 \times 34 - 1 \times (17 \times 34 - 4 \times 143)
\]

\[
= 5 \times 143 - 21 \times 34 \Rightarrow 34(-21) = 1 - 5(143)
\]

\( \Rightarrow 34^{-1} = -21 \mod 143 \), or \( x = -21 \)

Note: If I did not want to express the inverse as a negative number, I can add a multiple of 143

\( \Rightarrow 34^{-1} \equiv 122 \mod 143 \text{ or } x = 122 \)
Solving Systems of Congruences: Chinese Remainder Theory

Example:

\[
\begin{align*}
   x &\equiv 2 \mod 3 \quad \text{We need } \gcd(3,4) = 1 \\
   x &\equiv 2 \mod 4 \\
   x &\equiv 1 \mod 5
\end{align*}
\]

Idea: We will work out \( x \) in three sections

\[
\begin{align*}
   \mod 3 & \\
   \mod 4 & \\
   \mod 5 &
\end{align*}
\]

\[
x = ( \quad ) + ( \quad ) + ( \quad )
\]

To satisfy each of the congruences, I would like to ignore the remaining terms when considering the contribution of each term to \( x \).

\[
\implies \text{One way to do this is to include a multiplicative factor of each modulus to the remaining terms}
\]

\[
x = ( 4 \times 5 ) + ( 3 \times 5 ) + ( 3 \times 4 )
\]

\[
= 20 + 15 + 12
\]

Now, \( 20 \equiv 2 \mod 3 \quad \text{but} \quad 12 \equiv 1 \mod 5 \)

\[
12 \times 2 = 24 \equiv 1 \mod 5, \quad 12 \times 3 = 36 \equiv 1 \mod 5
\]

\[
\implies \text{we can include a multiplicative factor of } 3 \text{ to } 3^{\text{rd}} \text{ term}
\]

\[
15 \equiv 2 \mod 4, \quad 15 \times 2 = 2 \mod 4
\]

\[
\implies \text{we can include a multiplicative factor of } 2 \text{ to } 2^{\text{nd}} \text{ term}
\]

\[
= 4 \times 5 + 3 \times 5 \times 2 + 3 \times 4 \times 3 = 86 \equiv 2 \mod 3 \quad 2 \mod 4 \quad 1 \mod 5
\]

\[
\implies \text{an other way to express this is as } 26 \mod 60 \implies x = 26 \mod 60
\]
**EPR Proof**

Suppose $n_1, \ldots, n_k \in \mathbb{N}$ with $\gcd(n_i, n_j) = 1 \forall i \neq j$ and $b_1, \ldots, b_k \in \mathbb{Z}$.

Then the system of linear congruences

$$x \equiv b_i \mod n_i$$

$$x \equiv b_k \mod n_k$$

has a unique solution modulo $N = n_1 n_2 \cdots n_k$, where $N_i = \frac{N}{n_i}$.

**Proof**

Set $N = n_1 n_2 \cdots n_k$, Define $N_i = \frac{N}{n_i}$.

**Claim** $\gcd(N_i, n_i) = 1$

**Proof** Suppose $d | n_i$ and $d | N_i$.

$\Rightarrow$ Since all of the $n_i$'s relatively prime, $d$ must divide some $n_j \neq n_i$.

$\Rightarrow d | n_j$ for $j \neq i$

$\Rightarrow d | \gcd(n_j, n_i)$, $d | 1 \Rightarrow d = 1 \quad \Box$

$\gcd(N_i, n_i) = 1 \Rightarrow N_i$ has an inverse modulo $n_i$.

i) $\Rightarrow \exists x_i$ s.t. $N_i x_i \equiv 1 \mod n_i$ (possible by $\gcd(N_i, n_i) = 1$).

ii) $\Rightarrow x_i N_i \equiv 0 \mod n_j$ for $i \neq j$

because $N_i$ defined as product of little $n_i$'s except for $n_i$

$\Rightarrow N_i$ a multiple of $n_j \Rightarrow N_i \equiv 0 \mod n_j$
Consider \( x = x_1N_1b_1 + x_2N_2b_2 + \cdots + xKN_Kb_K \)
modulo \( n_i \); every term whose subscript \( i \) not equal to \( i \)
will be \( 0 \) from (ii) \( x_iN_i \equiv 0 \mod n_i \) \((i \neq j)\)
and \( 1 \) from (i) \( x_iN_i \equiv 1 \mod n_i \).

\[ \Rightarrow \exists x \equiv 0 + - + 0 + x_iN_ib_i + 0 + \pmod{n_i} \]

\[ x \equiv b_i \pmod{n_i} \quad 1 \leq i \leq K \quad \text{from (i)} \]

The \( N_i b_i \) are magic pairs modulo \( n_i \). This proves existence
of a solution \( a \).

**Uniqueness:** Sps \( x, y \) are sols

\[ \Rightarrow x \equiv b_i \pmod{n_i} \]

\[ y \equiv b_i \pmod{n_i} \]

\[ \Rightarrow x - y \equiv 0 \pmod{n_i} \quad 1 \leq i \leq K \]

\[ \Rightarrow n_i | (x - y) \Rightarrow x - y = c \cdot n_i \]

\[ \Rightarrow n_i \text{s are relatively prime,} \]

\[ N | x - y \]

\[ \Rightarrow x \equiv y \pmod{N} \]

(The solutions \( x, y \) are equivalent mod \( N \)) \( \square \)
Example: \( 4x \equiv 5 \mod 9 \)
\( 2x \equiv 6 \mod 20 \)

Here the setup is slightly different than as stated in CRT.
We can manipulate and put in form to apply and solve.

\[
4x \equiv 5 \mod 9
\]

Note \( \gcd(4, 9) = 1 \Rightarrow \) unique sol obtained by multiplying both sides
by multiplicative inverse of \( 4 \mod 9 \)

\[
4 \times 7 = 28 \equiv 1 \mod 9 \Rightarrow 7 = 4^{-1}
\]

\[\Rightarrow \text{Multiply both sides by 7:} \]
\[
x \equiv 35 \mod 9
\]
or
\[
x \equiv 8 \mod 9
\]

Now \( 2x \equiv 6 \mod 20 \). Note \( \gcd(2, 20) = 1 \), but all numbers even, so we can exploit this to write

\[
2x \equiv 2 \times 3 \mod 2 \times 10
\]

\[\Rightarrow \text{Now we can cancel the common factor from all of these parts} \]

\[\Rightarrow x \equiv 3 \mod 10 \]

Now the system can be reduced

\[\Rightarrow x \equiv 8 \mod 9 \Rightarrow N = 90 \quad N_1 = 10 \quad N_2 = 9
\]
\[x \equiv 3 \mod 10 \quad \text{Solve } N_1x_1 \equiv 1 \mod N_1
\]

\[
10x_1 \equiv 1 \mod 9 \Rightarrow x_1 \equiv 1 \mod 9, x_1 = 1
\]

\[
9x_2 \equiv 1 \mod 10 \Rightarrow 9x = 81 \equiv 1 \mod 10
\]

\[
x_2 = 9
\]

\[
x = \sum x_iN_i b_i = 1 \cdot 10 \cdot 8 + 9 \cdot 9 \cdot 3
\]

\[
x = 80 + 243 = 323
\]

\[\Rightarrow \text{should be unique } \mod 90 \Rightarrow 53 \mod 90
\]

\[
\begin{array}{c}
\text{but want to solve } \mod 180 \\
\text{want } x = \left[ 143 \mod 180 \right] \text{ (adding 90)}
\end{array}
\]

\[
x = 133 \mod 180
\]
For $a \in \mathbb{N}$, $p$ prime where $p \nmid a$

\[ a^{p-1} \equiv 1 \mod p \]

Ex: $p=5$, $a=2$ ($5 \times 2$) \[ p=3$, $a=4 \Rightarrow 3 \cdot 4 \equiv 1 \mod 5 \]

\[ 2 \equiv 1 \mod 5 \Rightarrow 2^4 = 16 \equiv 1 \mod 5 \]

**Proof**

All residues $\mod p$ are the numbers $\mod p$

Any number must fall in one of these equivalence classes

$\Rightarrow$ any $a \pmod{p}$ must be one of $0, 1, \ldots, p-1$

$\Rightarrow$ since $p \nmid a$, $a \notin [0]_p$

$a$ cannot be in congruence class of $0$

$\Rightarrow a \notin \{1, \ldots, p-1\}$

**Remark**

Multiplying $1, \ldots, p-1$ by any $a \in \mathbb{N}$

preserves the uniqueness of the congruence classes

and does not change the residues

Ex: $a=8$, $p=5$ \[ (1, 2, 3, 4) \times 8 = 8, 16, 24, 32 \]

$\mod 5 \Rightarrow 3, 1, 4, 2 \pmod{5} \Rightarrow 8, 16, 24, 32$

$\Rightarrow a \cdot (1, 2, \ldots, p-1) \equiv 1, 2, \ldots, p-1 \mod p$

$\Rightarrow a, 2a, 3a, \ldots, (p-1) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \mod p$

$\Rightarrow a^{p-1}(p-1)! \equiv (p-1)! \mod p$

Note $p \nmid (p-1)!$ \Rightarrow we can cancel \Rightarrow $a^{p-1} \equiv 1 \mod p$
However, two necklaces that are mirror images are different if they cannot be rotated.

Here, B should come before C.

We want to show the total # of necklaces is $\frac{4^7 - 4}{7}$.

$\Rightarrow$ # different necklaces must be an integer.

$\Rightarrow$ For this to be the case $7 | 4^7 - 4$ (which is what we want to prove).

Counting Necklaces:

Cut each necklace 4 straightly 1 out.

$\Rightarrow$ DAABCD

Q: There are other ways to cut the necklace, producing different strings.

$\Rightarrow$ 7 gaps b/t beads so 7 ways of cutting string (7 possible strings).

$\Rightarrow$ 7 different strings of beads:

A A B C D D D
A B C D D D A
B C D D D A A
C D D D A A B
D D D A A B C
D D A A B C D

But one color neckless A B B B B B B

How many 1 color neckless

$\Rightarrow 4^7 - 4$ strings possible

Every necklace gives rise to 7 strings
Total # strings:
7 beads, each 4 colors
\[4 \times 4 \times 4 \times 4 \times 4 \times 4 \times 4 = 4^7\]

But same color necklaces forbidden
\[\Rightarrow \text{How many one-color necklaces? 4}\]
\[\Rightarrow 4^7 - 4 \text{ strings}\]

Also every necklace under consideration gives rise to 7
different strings
\[\Rightarrow \# \text{different necklaces} = \frac{4^7 - 4}{7}\]

Q: Something weird in this proof.
At no point did we use the fact that 7 prime
\[\Rightarrow \text{If we replace prime \# 7 by composite \#, then not all}\]
strings that we get by rotating a necklace are necessarily
different.
\[\Rightarrow \text{we needed 7 different strings \# each necklace}\]
to justify our counting argument.

\[\times \text{ use 9 bends}\]
\[C \rightarrow A \rightarrow B \rightarrow C \rightarrow B \rightarrow A \rightarrow C \rightarrow B \rightarrow A\]

Things repeat every 3 bends when we cut necklace in all
possible ways, we get 3 different
strings, not 9

Q: Can this periodic necklace occur if it has prime # of beads?
   (and at least 2 colors)