Theorem: If \( a_1, a_2, \ldots, a_n \) are non-zero integers, then the equation \( a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \), has an integral solution \((c \in \mathbb{Z})\) if and only if \( d = (a_1, a_2, \ldots, a_n) \) divides \( c \). Furthermore, when there is a solution, there are infinitely many solutions.

Example: A grocer orders apples and oranges at a total cost of $8.39. If apples cost him 25¢ each and oranges cost 18¢ each, how many of each type of fruit did he order?

Answer: Let \( y \) = no. of oranges, \( x \) = no. of apples.

Total cost \( 25x + 18y = 839 \)

\( (25, 18) = 1 \), \( 1 \mid 139 \), hence solvable.

Using Euclidean algorithm, we find that

\(-5 \cdot 25 + 7 \cdot 18 = 1\)

\( x_0 = -5, y_0 = 7 \) is a solution.

But the solution has to be positive or nonnegative integers.
General solution:

\[ x = x_0 + \left( \frac{b}{d} \right) \, k, \quad y = y_0 + \left( \frac{c}{d} \right) \, k, \quad k \in \mathbb{Z} \]

\[ d = 1, \quad b = 18, \quad c = 25 \]

\[ -5 \cdot 25 + 7 \cdot 18 = 1 \]

\[ \Rightarrow \quad 25 \left( -5 \times 8.39 \right) + 18 \left( 7 \times 8.39 \right) = 839 \]

\[ \Rightarrow \quad 25 \left( -419.5 \right) + 18 \left( 587.3 \right) = 839 \]

\[ x_0 = -419.5, \quad y_0 = 587.3 \text{ is a solution.} \]

We want solutions to be non-negative.

General solution:

\[ x = -419.5 + 18 \, k, \quad y = 587.3 + 25 \, k, \quad k \in \mathbb{Z} \]

Want to choose \( k \) such that \( x \) and \( y \) are positive (\( x \geq 0, \quad y \geq 0 \)).

Solve for \( k \), then we find that

\[ 233 \leq k < 235 \]

So \( k = 234 \) works.
**Congruences:** Let $m$ be a positive integer. If $a, b \in \mathbb{Z}$, say that $a$ is **congruent to $b$ modulo $m$** if $m \mid (a - b)$.

*Example:* $18 \equiv 2 \mod 4$, $42 \equiv 7 \mod 5$

$130 \not\equiv 2 \mod 3$ since 128 is not divisible by 3.

**Theorem:** If $a, b \in \mathbb{Z}$, then $a \equiv b \mod m$ if and only if there is an integer $k$ s.t. $a = b + km$.

**Proof:** (We will also use the notation $a \equiv b \ (m)$ to denote $a \equiv b \mod m$).

$\Rightarrow$: Given $a \equiv b \mod m$, hence $m \mid (a - b)$.

$\Rightarrow a - b = km$ for some $k \in \mathbb{Z}$.

$\Rightarrow a = b + km$.

$\Leftarrow$: Given $a = b + km$. Hence $a - b = km$.

$\Rightarrow m \mid (a - b)$.

*Example:* $18 \equiv 2 \mod 4 \Rightarrow 18 = 16 + 2 = 4 \cdot 4 + 2$

$16 = (18 - 2)$, $4 \mid 16$, $k = 4$. 
Theorem: Let \( m \in \mathbb{Z}^+ \). Then congruences satisfy the following properties:

1. Reflexive property: If \( a \in \mathbb{Z} \), then \( a \equiv a \ (m) \).
2. Symmetry: If \( a, b \in \mathbb{Z} \) and \( a \equiv b \ (m) \), then \( b \equiv a \ (m) \).
3. Transitive: If \( a, b, c \in \mathbb{Z} \) and \( a \equiv b \ (m) \), \( b \equiv c \ (m) \), then \( a \equiv c \ (m) \).

Proof:

1. \( m \mid a-a = 0 \)
2. \( a \equiv b \ (m) \Rightarrow m \mid a-b \Rightarrow m \mid (b-a) \Rightarrow b \equiv a \ (m) \).
3. \( a \equiv b \ (m) \Rightarrow m \mid a-b, \ b \equiv c \ (m) \Rightarrow m \mid b-c \)

To show \( m \mid a-c \):

\[
\begin{align*}
a-c &= (a-b) + (b-c) \\
&= \equiv m \mid a-c \\
&\Rightarrow a \equiv c \ (m).
\end{align*}
\]

\( m \in \mathbb{Z}^+ \)

The set of integers is divided into \( m \) different equivalence classes modulo \( m \).

Each class contains all integers that are congruent modulo \( m \).
\[ \text{If } m = 2 \begin{cases} \text{even } \equiv 0 \mod 2, \\ \text{odd } \equiv 1 \mod 2. \end{cases} \]

In general, given \( m \in \mathbb{Z}^+ \), using the division algorithm, we know that there are \( m \) possible remainders when divided by \( m \), namely \( r \) such that \( 0 \leq r \leq m-1 \).

\[ \text{If } m = 4: \text{ The congruence classes are denoted } [0], [1], [2], [3]. \]

[0]: \( \{-8, -4, 0, 4, 8, 16, 20, \ldots \} = [4] \)

[1]: \( \{-7, -3, 1, 5, 9, 13, 21, \ldots \} = [-3] \)

[2]: \( \{-6, -2, 2, 6, 10, 14, 18, 22, \ldots \} = [-6] \)

[3]: \( \{-5, -1, 3, 7, 11, 15, 19, \ldots \} = [-1] \).

These remainders or congruence elements are called residues \( \mod m \).

Working with congruence classes is called Modulus Arithmetic.
Modular Arithmetic

Theorem: If \( a, b, c \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \) s.t. \( a \equiv b \pmod{m} \),
then:
1. \( a + c \equiv b + c \pmod{m} \)
2. \( a - c \equiv b - c \pmod{m} \)
3. \( ac \equiv bc \pmod{m} \)

Proof:
1. \( a \equiv b \pmod{m} \rightarrow m \mid a - b \rightarrow m \mid (a - b)c \)
2. \( a \equiv b \pmod{m} \rightarrow m \mid a - b \rightarrow m \mid (a - b)c \)
3. \( a \equiv b \pmod{m} \rightarrow m \mid a - b \rightarrow m \mid (a + c) - (b + c) \)
   \[ (a + c) - (b + c) = a - b, \text{ hence } m \mid (a + c) - (b + c) \]
   \[ \Rightarrow a + c \equiv b + c \pmod{m} \]

Example:
- \( -5 \equiv 3 \pmod{4} \) as \( (-5 - 3) = -8 \) and \( 4 \mid -8 \)

\[ 7 \equiv 3 \pmod{4} \]

Given:
- \( -5 \equiv 3 \pmod{4} \), \( 7 \equiv 3 \pmod{4} \)
- \( -5 + 1 \equiv 3 + 1 \pmod{4} \)
- \( 7 \times 2 = 14 \) and \( 3 \times 2 = 6 \)
- \( -4 \equiv 4 \pmod{4} \)
- \( 14 \equiv 6 \pmod{4} \) as \( 14 - 6 = 8 \) and \( 4 \mid 8 \)

Def: The congruence classes \( \mod{m} \) are called Residues modulo \( m \).
Theorem: If \( a, b \in \mathbb{Z}, m \in \mathbb{Z}^+ \), then \( a \equiv b \pmod{m} \) if and only if \([a] = [b]\).

Eq: \( 18 \mod 4 \); remainder = 2
\[
\begin{align*}
18 & \equiv 2 \pmod{4} \quad \text{and} \quad 18 - 22 = -4 \\
22 & \equiv 2 \pmod{4}
\end{align*}
\]

Def: A **complete system of residues modulo m** (\( m \in \mathbb{Z}^+ \)) is a set of integers such that every integer \( a \in \mathbb{Z} \) is congruent modulo \( m \) to exactly one integer in the given set.

Eq: \( \{0, 1, 2, \ldots, m-1\} \) is a complete system of residues \( \mod m \). This set is called the set of **least non-negative residues** \( \mod m \).

Eq: \( \{2m, 2m+1, 2m+2, \ldots, 2m+m-1\} \) is also a complete system of residues.

Rem: Cannot "cancel" and still preserve congruences.
\[ \begin{align*}
24 &\equiv 4 \mod 5 \Rightarrow 24 \equiv 2 \cdot 2 \mod 5 \\
24 &\equiv 4 \mod 5 \Rightarrow 24 \equiv 12 \cdot 2 \mod 5 \\
12 &\equiv 2 \mod 5 \quad \text{and} \quad 2 \cdot 12 \equiv 2 \cdot 2 \mod 5.
\end{align*} \]

\[ \begin{align*}
22 &\equiv 2 \cdot 2 \mod 6 \quad (22 = 4 \cdot 6) \\
22 &\equiv 5 \cdot 2 \mod 6 \quad (22-10 = 12 \cdot 6/12) \\
2 \cdot 2 &\equiv 5 \cdot 2 \mod 6 \quad \text{Cannot Cancel 2!} \\
2 &\not\equiv 5 \mod 6 \quad \text{as} \quad 2 - 5 = -3 \quad \text{and} \quad -3 \quad \text{is not divisible by 6.}
\end{align*} \]

**Theorem:** If \( a, b, c, m \in \mathbb{Z} \) and \( m \in \mathbb{Z}^+ \), \( d = (c, m) \) and \( ac \equiv bc \mod (m) \), then \( a \equiv b \mod \left( \frac{m}{d} \right) \).

**Proof:** Given \( ac \equiv bc \mod (m) \Rightarrow m \mid ac - bc = c(a-b) \);
\( \therefore c(a-b) = m \cdot k \). Need to show \( m \mid a-b \).

Since \( d = (c, m) \), we have \( d \mid c \) and \( d \mid m \)

\( \Rightarrow c = n_1 \cdot d \quad \text{and} \quad m = n_2 \cdot d \Rightarrow n_1 = \frac{c}{d} \quad \text{and} \quad n_2 = \frac{m}{d} \).

Know \( c(a-b) = m \cdot k \Rightarrow n_1 d(a-b) = n_2 d \cdot k \).

But \( \left( \frac{c}{d}, \frac{m}{d} \right) = 1 \Rightarrow \frac{m}{d} \mid a-b \) since

\[ n_1 d(a-b) = mk \Rightarrow a \equiv b \mod \left( \frac{m}{d} \right). \]
\[ \text{Cos: If } a, b, c \text{ and } m \in \mathbb{Z}, m \in \mathbb{Z}^+, \text{ and } (c, m) = 1 \text{ with } \]
\[ ac \equiv bc \ (m), \text{ then } a \equiv b \ (m). \]

\[ \text{Eg: } 24 \equiv 14 \mod 5 \implies 2, 12 \equiv 2, 7 \ (5) \]
\[ \text{But } (2, 5) = 1, \text{ hence } 12 \equiv 7 \ (5). \]

\[ \text{Theorem: If } a, b, c, d, m \in \mathbb{Z}, m \in \mathbb{Z}^+, \text{ and } a \equiv b \ (m), \]
\[ c \equiv d \ (m), \text{ then } a+c \equiv b+d \ (m), \]
\[ a-c \equiv b-d \ (m) \]
\[ \text{and } ac \equiv bd \ (m). \]

\[ \text{Proof: (i) } q \equiv b \ (m) \implies m|a-b, \]
\[ \text{hence } m|(a-b)+(c-d) \]
\[ c \equiv d \ (m) \implies m|c-d \implies m|(a+c)-(b+d) \]
\[ \implies a+c \equiv b+d \ (m). \]

(2) Similar:
(3) \[ m|a-b, \ m|c-d, \ m^2|ac-bd \]

\[ ac-bd = ac-bc+bc-bd \]
\[ = c(a-b)+b(c-d) \]
\[ m|a-b \text{ and } m|c-d \implies m|(a-b)+(c-d) \]
\[ \implies m|ac-bd \implies ac \equiv bd \ (m). \]

\[ \text{Theorem: A set of } m \text{ incongruent non-zero integers modulo } m \]
\[ \text{form a complete set of residues modulo } m. \]
Theorem: If \( \gamma_1, \gamma_2, \ldots, \gamma_m \) is a complete system of residues mod \( m \), and if \( \alpha \in \mathbb{Z}^+ \) with \( (\alpha, m) = 1 \), then \( (a\gamma_1+b, a\gamma_2+b, \ldots, a\gamma_m+b) \) is a complete system of residues mod \( m \).

**Proof.** By the previous theorem, enough to show that for \( i \neq j \), \( a\gamma_i+b \not\equiv a\gamma_j+b \) (mod \( m \)).

Suppose \( a\gamma_i+b \equiv a\gamma_j+b \) (mod \( m \)). Then \( a\gamma_i \equiv a\gamma_j \) (mod \( m \)). Since \( (\alpha, m) = 1 \), get \( \gamma_i \equiv \gamma_j \) (mod \( m \)) for \( i \neq j \).

\[ \Rightarrow \] Since \( \gamma_1, \ldots, \gamma_m \) is a complete system of residues. Hence \( a\gamma_i+b \not\equiv a\gamma_j+b \) (mod \( m \)) and the set \( \{a\gamma_i+b\}_{1 \leq i \leq m} \) is a complete system of residues.

**Theorem:** If \( a, b, k, m \in \mathbb{Z} \), \( m \in \mathbb{Z}^+ \), \( k > 0 \), and \( a \equiv b \) (mod \( m \)), then \( a^k \equiv b^k \) (mod \( m \)).

\[ (a^k - b^k) = (a-b)(a^{k-1} + ba^{k-2} + \ldots + ab^{k-2} + b^{k-1}) \]

\[ m | a-b \Rightarrow m | a^k - b^k \Rightarrow a^k \equiv b^k \) (mod \( m \)).

\[ \exists \quad 5 \equiv 2 \) (mod \( 3 \)); \[ 5^3 = 125 \equiv 2^3 = 8 \) (mod \( 3 \)), \[ 125 - 8 = 117 \]
and \( 3 | 117 \).
**FAST MODULAR EXPONENTIATION:**

*Goal:* Use Modular Arithmetic to find residues of large numbers (typically exponential) when divided by another number.

*Eg:* Find the residue of $5^{16} \mod 17$.

*Ans:* To find $x$ where $5^{16} \equiv x \mod 17$.

\[ 5^2 = 25 \equiv 8 \ (17) \ ; \text{so get by squaring} \]

\[ 5^4 \equiv 8^2 \ (17) \implies 5^4 \equiv 64 \ (17) \equiv -4 \ (17) \]

\[ \implies 5^8 \equiv -4 \ (17) \implies 5^8 \equiv 16 \ (17) \equiv -1 \ (17) \]

\[ \implies 5^{16} \equiv -1 \ (17) \implies 5^{16} \equiv 1 \ (17) \]

*Eg:* Find the residue of $3^{22} \mod 23$.

\[ 3^3 \equiv 27 \ (23) \equiv -4 \ (23) \]

Cube both sides to get,

\[ (3^3)^3 \equiv (-4)^3 \ (23) \equiv -64 \ (23) \equiv -5 \ (23) \]

\[ 3^9 \equiv -5 \ (23) ; \text{squaring we get} \]

\[ (3^9)^2 = 3^{18} \equiv (-5)^2 \ (23) \implies 3^{18} \equiv 25 \ (23) \implies 3^{18} \equiv 2 \ (23) \]

\[ 3^4 \equiv 3 \times 3^2 = 9 \times 9 = 81 \equiv 12 \ (23) \]
\[3^{18} \equiv 2 \mod 23, \quad 3^4 \equiv 12 \mod 23\]

Multiply both sides correspondingly to get,
\[3^{18} \cdot 3^4 \equiv 2 \cdot 12 \mod 23 \Rightarrow 3^2 \equiv 24 \mod 23 \equiv 1 \mod 23\]

Hence residue of \(3^{18} \mod 23 = 1\).

**Def:** A linear congruence in one variable is a congruence of the form \(ax \equiv b \mod m\), where \(x\) is an unknown.

**Observe:** Suppose \(x_0\) is a solution so that \(ax_0 \equiv b \mod m\) implies \(m \mid ax_0 - b\).

Suppose \(x_1 \equiv x_0 \mod m\) so that \([x_1] = [x_0]\).

\[\Rightarrow m \mid x_1 - x_0 \Rightarrow m \mid ax_1 - ax_0\]

\[\Rightarrow m \mid ax_1 - ax_0 + ax_0 - b \Rightarrow m \mid ax_1 - b\]

Hence the whole congruence class of \(x_0\) gives us solutions, so we can talk of "congruence class" solutions to a linear congruence.

Same as asking, how many "incongruent" solutions exist, i.e., how many solutions \(x_i\) satisfy the equation \(ax_i \equiv b \mod m\) and \(x_i \neq x_j \mod m\) if \(i \neq j\).
Theorem: Let \( a, b \) and \( m \) be integers, \( m > 0 \) and \( (a, m) = d \).

If \( d \nmid b \), then \( ax \equiv b \pmod{m} \) has no solution.

If \( d \mid b \), then \( ax \equiv b \pmod{m} \) has exactly \( d \) incongruent solutions \( \pmod{m} \).

\[ \text{Ex: } 3x \equiv 4 \pmod{6}; \ a = 3, \ b = 4, \ m = 6, \]
\[ (a, m) = (3, 6) = 3 = d. \text{ Note } 3 \nmid 4. \]

Hence no solutions.

\[ \text{Ex: } 4x \equiv 2 \pmod{6}; \ a = 4, \ b = 2, \ m = 6, \]
\[ (a, m) = (4, 6) = 2 = d, \ 2 \mid 2 \checkmark \]

So solutions exist.

- Infinitely many solutions that are congruent.
- Finitely many incongruent solutions, \( 2 \) incongruent solutions.

\[ 4x \equiv 2 \pmod{6}; \ x_0 = 2 \] is a solution.

The other incongruent solutions: Look among \( x_0 + dk, \ k \in \mathbb{Z}; \ 2 + 2k, \ k = 0, 1, 2, 3, 4, 5 \).

\[ 4 \cdot 5 = 20 \equiv 2 \pmod{6} \text{ as } 6 \mid 18. \]

- If \( x_0 \) is a solution, there are infinitely many congruent solutions \( x = x_0 + (\frac{m}{d})k, \ k \in \mathbb{Z} \).
- Incongruent solutions: \( x = x_0 + (\frac{m}{d})k, \ k \) varies over a complete set of residues \( \pmod{m} \).
Theorem: Let \( p \) be a prime. The positive integer \( a \) is its own inverse \( \text{mod} \ p \) if and only if \( a \equiv 1 \ (p) \) or \( a \equiv -1 \ (p) \).

**Proof:**

\( \Rightarrow \): Suppose \( a \equiv 1 \ (p) \) or \( a \equiv -1 \ (p) \).

This means that \( p \mid a - 1 \) or \( p \mid a + 1 \).

So \( p \mid (a - 1)(a + 1) \Rightarrow p \mid a^2 - 1 \Rightarrow a^2 \equiv 1 \ (p) \Rightarrow \bar{a} \text{ is the modular inverse of} \ a \text{ mod} \ p = a \).

\( \Rightarrow \): Given \( \bar{a} \equiv a \ (p) \Rightarrow a \cdot a \equiv 1 \ (p) \),

\( \Rightarrow \ a^2 \equiv 1 \ (p) \Rightarrow p \mid a^2 - 1 \),

\( \Rightarrow p \mid (a - 1)(a + 1). \) But \( p \) is a prime,

hence \( p \mid (a - 1) \) or \( p \mid (a + 1) \).

\( \Rightarrow a \equiv 1 \ (\text{mod} \ p) \) or \( a \equiv -1 \ (p) \).

\( \exists \): \( p = 5; \ a = 6 \) : \( a^2 = 36, \ 36 \equiv 1 \ (5) \)

\( a = 4 : \ 4^2 = 16 \equiv 1 \ (5) \) \( \left| \begin{array}{c} 6 \equiv 1 \ (5) \\
4 \equiv -1 \ (5)
\end{array} \right| \)