Lecture 7 Outline.

1. Modular Arithmetic.
Lecture 7 Outline.

1. Modular Arithmetic.
   Clock Math!!!
Lecture 7 Outline.

1. Modular Arithmetic.
   Clock Math!!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor (GCD).
3. Euclid’s GCD Algorithm
Clock Math

If it is 4:00 now.
If it is 4:00 now.
What time is it in 5 hours?
If it is 4:00 now.
What time is it in 5 hours? 9:00!
Clock Math

If it is 4:00 now.
   What time is it in 5 hours? 9:00!
   What time is it in 15 hours?
Clock Math

If it is 4:00 now.
   What time is it in 5 hours? 9:00!
   What time is it in 15 hours? 19:00!
Clock Math

If it is 4:00 now.
  What time is it in 5 hours? 9:00!
  What time is it in 15 hours? 19:00!
    Actually 7:00.
If it is 4:00 now.

What time is it in 5 hours? 9:00!
What time is it in 15 hours? 19:00!
Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock Math

If it is 4:00 now.
  What time is it in 5 hours? 9:00!
  What time is it in 15 hours? 19:00!
    Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.
If it is 4:00 now.
    What time is it in 5 hours? 9:00!
What time is it in 15 hours? 19:00!
    Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to addition/subtraction of 12.
If it is 4:00 now.
  What time is it in 5 hours? 9:00!
  What time is it in 15 hours? 19:00!
    Actually 7:00.

  19 is the “same as 7” with respect to a 12 hour clock system.
  Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours?
Clock Math

If it is 4:00 now.
  What time is it in 5 hours? 9:00!
  What time is it in 15 hours? 19:00!
    Actually 7:00.

  19 is the “same as 7” with respect to a 12 hour clock system.
    Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 104:00!
If it is 4:00 now.
   What time is it in 5 hours? 9:00!
   What time is it in 15 hours? 19:00!
      Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 104:00! or 8:00.
If it is 4:00 now.

What time is it in 5 hours? 9:00!
What time is it in 15 hours? 19:00!
Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to addition/subtraction of 12.

What time is it in 100 hours? 104:00! or 8:00.
8 is the same as 104 for a 12 hour clock system.
If it is 4:00 now.
   What time is it in 5 hours? 9:00!
   What time is it in 15 hours? 19:00!
       Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
   Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 104:00! or 8:00.
   8 is the same as 104 for a 12 hour clock system.
       Clock time equivalent up to addition of any integer multiple of 12.
If it is 4:00 now.
   What time is it in 5 hours? 9:00!
   What time is it in 15 hours? 19:00!
   Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to to addition/subtraction of 12.

What time is it in 100 hours? 104:00! or 8:00.
8 is the same as 104 for a 12 hour clock system.
Clock time equivalent up to addition of any integer multiple of 12.
If it is 4:00 now.
    What time is it in 5 hours? 9:00!
    What time is it in 15 hours? 19:00!
    Actually 7:00.

19 is the “same as 7” with respect to a 12 hour clock system.
Clock time equivalent up to addition/subtraction of 12.

What time is it in 100 hours? 104:00! or 8:00.
    8 is the same as 104 for a 12 hour clock system.
    Clock time equivalent up to addition of any integer multiple of 12.

Custom is only to use the representative in \{1, \ldots, 11, 12\}
Today is Tuesday.
Today is Tuesday.
What day is it a year from now?
Today is Tuesday.

What day is it a year from now? on February 6, 2025?
Day of the week.

Today is Tuesday. What day is it a year from now? on February 6, 2025? Number days.
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
  0 for Sunday, 1 for Monday, . . . , 6 for Saturday.
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.

4 days from now.
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
  0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
  4 days from now. day 6
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

  0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.

  4 days from now. day 6 or Saturday.
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now.

This year is a leap year!

So 366 days from now.
Day 2+366 or day 368.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
368/7 leaves quotient of 52 and remainder 4.
or February 6, 2025 is Day 4, a Thursday.
Day of the week.

Today is Tuesday.
  What day is it a year from now? on February 6, 2025?
  Number days.
    0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
  4 days from now. day 6 or Saturday.
  24 days from now. day 26
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.

4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
Day of the week.

Today is Tuesday.
   What day is it a year from now? on February 6, 2025?
   Number days.
      0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
   4 days from now. day 6 or Saturday.
   24 days from now. day 26 or day 5, which is Friday!
      two days are equivalent up to addition/subtraction of multiple of 7.
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.

4 days from now. day 6 or Saturday.

24 days from now. day 26 or day 5, which is Friday!

two days are equivalent up to addition/subtraction of multiple of 7.

10 days from now
Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.

4 days from now. day 6 or Saturday.

24 days from now. day 26 or day 5, which is Friday!

two days are equivalent up to addition/subtraction of multiple of 7.

10 days from now is day 5 again, Friday!
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?

Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
    two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year!
Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
  0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
  4 days from now. day 6 or Saturday.
  24 days from now. day 26 or day 5, which is Friday!
  two days are equivalent up to addition/subtraction of multiple of 7.
  10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.
0 for Sunday, 1 for Monday, \ldots, 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.
Today is Tuesday.

What day is it a year from now? on February 6, 2025?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.
Smallest representation:
Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

0 for Sunday, 1 for Monday, \ldots, 6 for Saturday.

Today: day 2.

4 days from now. day 6 or Saturday.

24 days from now. day 26 or day 5, which is Friday!

two days are equivalent up to addition/subtraction of multiple of 7.

10 days from now is day 5 again, Friday!

What day is it a year from now?

This year is a leap year! So 366 days from now.

Day 2+366 or day 368.

Smallest representation:

subtract 7 until smaller than 7.
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?

Number days.
 0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
 4 days from now. day 6 or Saturday.
 24 days from now. day 26 or day 5, which is Friday!
    two days are equivalent up to addition/subtraction of multiple of 7.
 10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.

Smallest representation:
  subtract 7 until smaller than 7.
  divide and get remainder.

or February 6, 2025 is Day 4, a Thursday.
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.

0 for Sunday, 1 for Monday, \ldots, 6 for Saturday.

Today: day 2.

4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!

two days are equivalent up to addition/subtraction of multiple of 7.

10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.

Day 2+366 or day 368.

Smallest representation:

subtract 7 until smaller than 7.

divide and get remainder.

368/7
Day of the week.

Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!

two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.

Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
368/7 leaves quotient of 52 and remainder 4.
Day of the week.

Today is Tuesday.
What day is it a year from now? on February 6, 2025?
Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
368/7 leaves quotient of 52 and remainder 4.
or February 6, 2025 is Day 4, a Thursday.
Today is Tuesday.

What day is it a year from now? on February 6, 2025?

Number days.
0 for Sunday, 1 for Monday, . . . , 6 for Saturday.

Today: day 2.
4 days from now. day 6 or Saturday.
24 days from now. day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
10 days from now is day 5 again, Friday!

What day is it a year from now?
This year is a leap year! So 366 days from now.
Day 2+366 or day 368.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
368/7 leaves quotient of 52 and remainder 4.
or February 6, 2025 is Day 4, a Thursday.
Years and years...

80 years from now? February 6, 2104
20 leap years. 366*20 days
60 regular years. 365*60 days
It is day \(2 + 366 \times 20 + 365 \times 60\). Equivalent to?

Hmm.

What is remainder of 366 when dividing by 7? 2.
What is remainder of 365 when dividing by 7? 1

Today is day 2.
Get Day: \(2 + 20 \times 2 + 60 \times 1 = 102\)
Remainder when dividing by 7? 4.
Or February 6, 2104 is Thursday!

Further Simplify Calculation:
20 has remainder 6 when divided by 7.
60 has remainder 4 when divided by 7.
Get Day: \(2 + 6 \times 2 + 4 \times 1 = 18\).
Or Day 4. February 6, 2104 is Thursday.

“Reduce” at any time in calculation!
Modular Arithmetic: Basics.

\( x \) is congruent to \( y \) modulo \( m \) or “\( x \equiv y \ (\text{mod } m) \)” if and only if \( (x - y) \) is divisible by \( m \).
Modular Arithmetic: Basics.

\[ x \text{ is congruent to } y \text{ modulo } m \text{ or } “x \equiv y \text{ (mod } m\text{)” } \]

if and only if \((x - y)\) is divisible by \(m\).

...or \(x = y + km\) for some integer \(k\).
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.
...or $x = y + km$ for some integer $k$.
...or $x$ and $y$ have the same remainder w.r.t. $m$. 
Modular Arithmetic: Basics.

\[ x \text{ is congruent to } y \text{ modulo } m \text{ or } \left( x \equiv y \pmod{m} \right) \]
if and only if \((x - y)\) is divisible by \(m\).
...or \(x = y + km\) for some integer \(k\).
...or \(x\) and \(y\) have the same remainder w.r.t. \(m\).
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or "$x \equiv y \pmod{m}$" if and only if $(x - y)$ is divisible by $m$.
...or $x = y + km$ for some integer $k$.
...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:
Modular Arithmetic: Basics.

\( x \) is congruent to \( y \) modulo \( m \) or “\( x \equiv y \) \( (\text{mod } m) \)” if and only if \( (x - y) \) is divisible by \( m \).

...or \( x = y + km \) for some integer \( k \).

...or \( x \) and \( y \) have the same remainder w.r.t. \( m \).

Mod 7 equivalence classes:
{\ldots, -7, 0, 7, 14, \ldots}
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.

...or $x = y + km$ for some integer $k$.

...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:

$\{\ldots, -7, 0, 7, 14, \ldots \}$  $\{\ldots, -6, 1, 8, 15, \ldots \}$
Modular Arithmetic: Basics.

\( x \) is congruent to \( y \) modulo \( m \) or “\( x \equiv y \pmod{m} \)” if and only if \((x - y)\) is divisible by \( m \).

...or \( x = y + km \) for some integer \( k \).

...or \( x \) and \( y \) have the same remainder w.r.t. \( m \).

Mod 7 equivalence classes:
\[
\{\ldots,-7,0,7,14,\ldots\} \quad \{\ldots,-6,1,8,15,\ldots\} \quad \ldots
\]
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.
...or $x = y + km$ for some integer $k$.
...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:
{\ldots, -7, 0, 7, 14, \ldots} {\ldots, -6, 1, 8, 15, \ldots} ...

**Useful Fact:** Addition, subtraction, multiplication can be done with any equivalent $x$ and $y$. 

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer $k$. If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer $j$. Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer. $\Rightarrow a + b \equiv c + d \pmod{m}$.

Can calculate with representative in {\ldots, 0, \ldots, m - 1}. 
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.

...or $x = y + km$ for some integer $k$.

...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:
{..., −7, 0, 7, 14,...}  {..., −6, 1, 8, 15,...} ...

**Useful Fact:** Addition, subtraction, multiplication can be done with any equivalent $x$ and $y$.

or “ $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$ ”
Modular Arithmetic: Basics.

\[ x \text{ is congruent to } y \text{ modulo } m \text{ or } "x \equiv y \pmod{m}" \]
if and only if \((x - y)\) is divisible by \(m\).
...or \(x = y + km\) for some integer \(k\).
...or \(x\) and \(y\) have the same remainder w.r.t. \(m\).

Mod 7 equivalence classes:
\{\ldots, -7, 0, 7, 14, \ldots\} \quad \{\ldots, -6, 1, 8, 15, \ldots\} \ldots

**Useful Fact:** Addition, subtraction, multiplication can be done with any equivalent \(x\) and \(y\).

or "\(a \equiv c \pmod{m}\) and \(b \equiv d \pmod{m}\)
\[ \implies a + b \equiv c + d \pmod{m} \text{ and } a \cdot b \equiv c \cdot d \pmod{m}" \]
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.

...or $x = y + km$ for some integer $k$.

...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:

$\{\ldots, -7, 0, 7, 14, \ldots\}$  $\{\ldots, -6, 1, 8, 15, \ldots\}$ ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent $x$ and $y$.

or “$a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$

$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b \equiv c \cdot d \pmod{m}$”

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer $k$. 

Modular Arithmetic: Basics.

\( x \) is congruent to \( y \) modulo \( m \) or \( \text{“} x \equiv y \pmod{m} \text{”} \)
if and only if \( (x - y) \) is divisible by \( m \).

...or \( x = y + km \) for some integer \( k \).

...or \( x \) and \( y \) have the same remainder w.r.t. \( m \).

Mod 7 equivalence classes:
\{ \ldots, -7, 0, 7, 14, \ldots \} \quad \{ \ldots, -6, 1, 8, 15, \ldots \} \ldots

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent \( x \) and \( y \).

or \( \text{“} a \equiv c \pmod{m} \) and \( b \equiv d \pmod{m} \)
\( \implies a + b \equiv c + d \pmod{m} \) and \( a \cdot b \equiv c \cdot d \pmod{m} \)”

Proof: If \( a \equiv c \pmod{m} \), then \( a = c + km \) for some integer \( k \).
If \( b \equiv d \pmod{m} \), then \( b = d + jm \) for some integer \( j \).
Modular Arithmetic: Basics.

x is congruent to y modulo m or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.
...or $x = y + km$ for some integer $k$.
...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:
{..., −7, 0, 7, 14,...}  {..., −6, 1, 8, 15,...} ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent $x$ and $y$.

or “ $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$

$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b \equiv c \cdot d \pmod{m}$”

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer $k$.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer $j$.
Therefore,
Modular Arithmetic: Basics.

*x is congruent to y modulo m* or “*x ≡ y (mod m)*” if and only if *(x − y)* is divisible by *m*.

...or *x = y + km* for some integer *k*.

...or *x* and *y* have the same remainder w.r.t. *m*.

Mod 7 equivalence classes:

{..., −7, 0, 7, 14, ...} {..., −6, 1, 8, 15, ...}...

**Useful Fact:** Addition, subtraction, multiplication can be done with any equivalent *x* and *y*.

or “*a ≡ c (mod m)* and *b ≡ d (mod m)*

⇒ *a + b ≡ c + d (mod m)* and *a · b = c · d (mod m)***”

**Proof:** If *a ≡ c (mod m)*, then *a = c + km* for some integer *k*.

If *b ≡ d (mod m)*, then *b = d + jm* for some integer *j*.

Therefore,  

\[ a + b = c + d + (k + j)m \]
Modular Arithmetic: Basics.

\( x \) is congruent to \( y \) modulo \( m \) or \( x \equiv y \pmod{m} \)
if and only if \( (x - y) \) is divisible by \( m \).
...or \( x = y + km \) for some integer \( k \).
...or \( x \) and \( y \) have the same remainder w.r.t. \( m \).

Mod 7 equivalence classes:
\{\ldots, -7, 0, 7, 14, \ldots\} \quad \{\ldots, -6, 1, 8, 15, \ldots\} \ldots

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent \( x \) and \( y \).

or \( \text{“} a \equiv c \pmod{m} \) and \( b \equiv d \pmod{m} \)

\[ \implies a + b \equiv c + d \pmod{m} \) and \( a \cdot b = c \cdot d \pmod{m} \)\]

Proof: If \( a \equiv c \pmod{m} \), then \( a = c + km \) for some integer \( k \).
If \( b \equiv d \pmod{m} \), then \( b = d + jm \) for some integer \( j \).
Therefore, \( a + b = c + d + (k + j)m \) and since \( k + j \) is integer.
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.
...or $x = y + km$ for some integer $k$.
...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:
{\ldots, -7, 0, 7, 14, \ldots} {\ldots, -6, 1, 8, 15, \ldots} ... 

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent $x$ and $y$.

or “$a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$

$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$”

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer $k$.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer $j$.
Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer.
$\implies a + b \equiv c + d \pmod{m}$. 
Modular Arithmetic: Basics.

**x is congruent to y modulo m** or “x ≡ y (mod m)”
if and only if (x − y) is divisible by m.
...or x = y + km for some integer k.
...or x and y have the same remainder w.r.t. m.

Mod 7 equivalence classes:
{..., −7, 0, 7, 14,...}   {..., −6, 1, 8, 15,...}  ...

**Useful Fact:** Addition, subtraction, multiplication can be done with
any equivalent x and y.

or “ a ≡ c (mod m) and b ≡ d (mod m)
⇒  a + b ≡ c + d (mod m) and a · b = c · d (mod m)”

**Proof:** If a ≡ c (mod m), then a = c + km for some integer k.
If b ≡ d (mod m), then b = d + jm for some integer j.
Therefore,  a + b = c + d + (k + j)m  and since k + j is integer.
⇒  a + b ≡ c + d (mod m).  □
Modular Arithmetic: Basics.

$x$ is congruent to $y$ modulo $m$ or “$x \equiv y \pmod{m}$” if and only if $(x - y)$ is divisible by $m$.
...or $x = y + km$ for some integer $k$.
...or $x$ and $y$ have the same remainder w.r.t. $m$.

Mod 7 equivalence classes:
{\ldots, -7, 0, 7, 14, \ldots}  {\ldots, -6, 1, 8, 15, \ldots} ...

Useful Fact: Addition, subtraction, multiplication can be done with any equivalent $x$ and $y$.

or “$a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$

$\implies a + b \equiv c + d \pmod{m}$ and $a \cdot b \equiv c \cdot d \pmod{m}$”

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some integer $k$.
If $b \equiv d \pmod{m}$, then $b = d + jm$ for some integer $j$.
Therefore, $a + b = c + d + (k + j)m$ and since $k + j$ is integer.
$\implies a + b \equiv c + d \pmod{m}$. □

Can calculate with representative in $\{0, \ldots, m-1\}$. 
Notation

\( x \ (\text{mod} \ m) \) or \( \text{mod} \ (x, m) \)- remainder of \( x \) divided by \( m \) in \( \{0, \ldots, m - 1\} \).
Notation

\[ x \pmod{m} \text{ or } \mod (x, m) - \text{ remainder of } x \text{ divided by } m \text{ in } \{0, \ldots, m - 1\}. \]
Notation

\[ x \pmod{m} \text{ or } \text{mod} \ (x, m) - \text{remainder of } x \text{ divided by } m \text{ in } \{0, \ldots, m - 1\}. \]

\[ \text{mod} \ (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m \]
Notation

$x \ (\text{mod } m)$ or $\text{mod} \ (x, m)$- remainder of $x$ divided by $m$ in \{0, \ldots, m - 1\}.

$\text{mod} \ (x, m) = x - \lfloor \frac{x}{m} \rfloor m$

$\lfloor \frac{x}{m} \rfloor$ is quotient.
Notation

\( x \pmod{m} \) or \( \text{mod } (x, m) \)- remainder of \( x \) divided by \( m \) in \( \{0, \ldots, m-1\} \).

\[ \text{mod } (x, m) = x - \lfloor \frac{x}{m} \rfloor m \]

\( \lfloor \frac{x}{m} \rfloor \) is quotient.

\[ \text{mod } (29, 12) = 29 - (\lfloor \frac{29}{12} \rfloor) \times 12 \]
Notation

\[ x \pmod{m} \] or \[ \text{mod} (x, m) \] - remainder of \( x \) divided by \( m \) in \( \{0, \ldots, m-1\} \).

\[ \text{mod} (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m \]

\[ \left\lfloor \frac{x}{m} \right\rfloor \] is quotient.

\[ \text{mod} (29, 12) = 29 - (\left\lfloor \frac{29}{12} \right\rfloor) \times 12 = 29 - (2) \times 12 \]
Notation

\( x \pmod{m} \) or \( \text{mod} \ (x, m) \)- remainder of \( x \) divided by \( m \) in \( \{0, \ldots, m-1\} \).

\[ \text{mod} \ (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m \]

\( \left\lfloor \frac{x}{m} \right\rfloor \) is quotient.

\[ \text{mod} \ (29, 12) = 29 - \left( \left\lfloor \frac{29}{12} \right\rfloor \right) \times 12 = 29 - (2) \times 12 = 5 \]
Notation

$x \ (\text{mod} \ m)$ or $\text{mod} \ (x, m)$ - remainder of $x$ divided by $m$ in $\{0, \ldots, m-1\}$.

$$\text{mod} \ (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m$$

$\left\lfloor \frac{x}{m} \right\rfloor$ is quotient.

$$\text{mod} \ (29, 12) = 29 - (\left\lfloor \frac{29}{12} \right\rfloor) \times 12 = 29 - (2) \times 12 = 5$$

Recap:
Notation

\( x \pmod{m} \) or \( \text{mod} (x, m) \) - remainder of \( x \) divided by \( m \) in \( \{0, \ldots, m-1\} \).

\[
\text{mod} (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m
\]

\( \left\lfloor \frac{x}{m} \right\rfloor \) is quotient.

\[
\text{mod} (29, 12) = 29 - \left(\left\lfloor \frac{29}{12} \right\rfloor\right) \times 12 = 29 - (2) \times 12 = 5
\]

Recap:

\( a \equiv b \pmod{m} \).
Notation

\( x \pmod{m} \) or \( \text{mod} \ (x, m) \) - remainder of \( x \) divided by \( m \) in \( \{0, \ldots, m-1\} \).

\[
\text{mod} \ (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m
\]

\( \left\lfloor \frac{x}{m} \right\rfloor \) is quotient.

\[
\text{mod} \ (29, 12) = 29 - \left(\left\lfloor \frac{29}{12} \right\rfloor \right) \times 12 = 29 - (2) \times 12 = 5
\]

Recap:

\( a \equiv b \pmod{m} \).

Says two integers \( a \) and \( b \) are equivalent modulo \( m \).
Notation

\( x \pmod{m} \) or \( \text{mod} (x, m) \)- remainder of \( x \) divided by \( m \) in \{0, \ldots, m-1\}.

\[
\text{mod} (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m
\]

\( \left\lfloor \frac{x}{m} \right\rfloor \) is quotient.

\[
\text{mod} (29, 12) = 29 - (\left\lfloor \frac{29}{12} \right\rfloor) \times 12 = 29 - (2) \times 12 = 5
\]

Recap:
\( a \equiv b \pmod{m} \).

Says two integers \( a \) and \( b \) are equivalent modulo \( m \).

**Modulus** is \( m \)
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1 \);
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1 \); **1 is multiplicative identity element.**
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies \left(\frac{1}{2}\right) \cdot 2x = \left(\frac{1}{2}\right)3 \implies x = 3/2. \]

**Multiplicative inverse of** \(x\) **is** \(y\) **where** \(xy = 1\); \(1\) **is multiplicative identity element.**

In modular arithmetic, \(1\) **is the multiplicative identity element.**
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1 \); 1 **is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) **is** \( y \) **with** \( xy = 1 \) (mod \( m \)).
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1; 1 \) is multiplicative identity element.

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \[ 2 \cdot 4 \equiv 8 \equiv 1 \mod 7. \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1; \)
**1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) **is** \( y \) with \( xy = 1 \mod m).**

For 4 modulo 7 inverse is 2: \[ 2 \cdot 4 \equiv 8 \equiv 1 \mod 7. \]
Can solve \( 4x = 5 \mod 7). \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1 \); 
**1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) **is** \( y \) **with** \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \( 2 \cdot 4 \equiv 8 \equiv 1 \mod 7 \).

Can solve \( 4x = 5 \mod 7 \).
\[ 2 \cdot 4x = 2 \cdot 5 \mod 7 \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1 \); 1 is multiplicative identity element.

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \( 2 \cdot 4 \equiv 8 \equiv 1 \mod 7 \).

Can solve \( 4x = 5 \mod 7 \).
\[ 2 \cdot 4x = 2 \cdot 5 \mod 7 \]
\[ 8x = 10 \mod 7 \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies \left(\frac{1}{2}\right) \cdot 2x = \left(\frac{1}{2}\right)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1 \); 
**1** is multiplicative identity element.

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \( 2 \cdot 4 \equiv 8 \equiv 1 \mod 7 \).

Can solve \( 4x = 5 \mod 7 \).
\[ 2 \cdot 4x = 2 \cdot 5 \mod 7 \]
\[ 8x = 10 \mod 7 \]
\[ x = 3 \mod 7 \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1 \); \( 1 \) is multiplicative identity element.

In modular arithmetic, \( 1 \) is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \( 2 \cdot 4 \equiv 8 \equiv 1 \mod 7 \).

Can solve \( 4x = 5 \mod 7 \).
\[
2 \cdot 4x = 2 \cdot 5 \mod 7 \\
8x = 10 \mod 7 \\
x = 3 \mod 7
\]

Check!
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1; \) **1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) **is** \( y \) **with** \( xy = 1 \mod m).**

For 4 modulo 7 inverse is 2: \( 2 \cdot 4 \equiv 8 \equiv 1 \mod 7). \)

Can solve \( 4x = 5 \mod 7). \)
\( 2 \cdot 4x = 2 \cdot 5 \mod 7) \)
\( 8x = 10 \mod 7) \)
\( x = 3 \mod 7) \)
Check! \( 4(3) = 12 = 5 \mod 7). \)
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1 \);

**1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2:

\[ 2 \cdot 4 \equiv 8 \equiv 1 \mod 7. \]

Can solve \( 4x = 5 \mod 7 \).

\( x = 3 \mod 7 \implies \text{Check! } 4(3) = 12 = 5 \mod 7. \)
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1 \);
1 is multiplicative identity element.

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2:
\[ 2 \cdot 4 \equiv 8 \equiv 1 \mod 7. \]
Can solve \( 4x = 5 \mod 7 \).
\[ x = 3 \mod 7 \implies \text{Check! } 4(3) = 12 = 5 \mod 7. \]

For 8 modulo 12: no multiplicative inverse!
Inverses and Factors.

Division: multiply by multiplicative inverse.

$$2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2.$$  

**Multiplicative inverse of** $x$ **is** $y$ **where** $xy = 1$; 
**1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element. 

**Multiplicative inverse of** $x \mod m$ **is** $y$ **with** $xy = 1 \mod m$.

For 4 modulo 7 inverse is 2:  
$$2 \cdot 4 \equiv 8 \equiv 1 \mod 7.$$  

Can solve $4x = 5 \mod 7$.  
$x = 3 \mod 7$ ::: Check! $4(3) = 12 = 5 \mod 7$. 

For 8 modulo 12: no multiplicative inverse!

“Common factor of 4”
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1 \);
**1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) **is** \( y \) **with** \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2:
\[ 2 \cdot 4 \equiv 8 \equiv 1 \mod 7. \]

Can solve \( 4x = 5 \mod 7 \).
\[ x = 3 \mod 7 \implies \text{Check! } 4(3) = 12 = 5 \mod 7. \]

For 8 modulo 12: no multiplicative inverse!

“Common factor of 4”
\[ 8k - 12\ell \text{ is a multiple of four for any } \ell \text{ and } k \implies \]
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) **is** \( y \) **where** \( xy = 1 \); 1 is multiplicative identity element.

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) **is** \( y \) **with** \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \[ 2 \cdot 4 \equiv 8 \equiv 1 \mod 7. \]

Can solve \( 4x = 5 \mod 7 \). \[ x = 3 \mod 7 \] : Check! \( 4(3) = 12 = 5 \mod 7 \).

For 8 modulo 12: no multiplicative inverse!

“Common factor of 4” \( \implies \)
\( 8k - 12\ell \) **is** a **multiple** **of** **four for any** \( \ell \) **and** \( k \) \( \implies \)
\( 8k \not\equiv 1 \mod 12 \) for any \( k \).
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$. 

Proof $\Rightarrow$:
The set $S = \{0 \cdot x, 1 \cdot x, \ldots, (m-1) \cdot x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$.

*Pigeonhole principle:* Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\Rightarrow$ One must correspond to 1 modulo $m$. If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where $(ax \equiv bx \pmod{m}) \Rightarrow (a - b) \cdot x \equiv 0 \pmod{m}$

$\gcd(x, m) = 1 \Rightarrow$ Prime factorization of $m$ and $x$ do not contain common primes. $\Rightarrow$ $(a - b)$ factorization contains all primes in $m$’s factorization.

$\Rightarrow$ $(a - b)$ has to be multiple of $m$.

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

But $a, b \in \{0, \ldots, m-1\}$.

Contradiction.
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of \( x \) and \( m \), \( \gcd(x, m) \), is 1, then \( x \) has a multiplicative inverse modulo \( m \).

**Proof** \( \implies \): The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).
**Greatest Common Divisor and Inverses.**

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof $\iff$:** The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

**Pigenhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$. 
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof $\Rightarrow$:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\Rightarrow$ One must correspond to 1 modulo $m$. 
Greatest Common Divisor and Inverses.

Thm: If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

Pigeonhole principle: Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$,
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof** $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where $(ax \equiv bx \mod m) \implies (a - b)x \equiv 0 \mod m$
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of \( x \) and \( m \), \( \gcd(x, m) \), is 1, then \( x \) has a multiplicative inverse modulo \( m \).

**Proof** \( \Rightarrow \): The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

**Pigeonhole principle:** Each of \( m \) numbers in \( S \) correspond to different one of \( m \) equivalence classes modulo \( m \).
\[ \Rightarrow \text{ One must correspond to } 1 \text{ modulo } m. \]

If not distinct, then \( a, b \in \{0, \ldots, m - 1\} \), where
\[ (ax \equiv bx \pmod{m}) \Rightarrow (a - b)x \equiv 0 \pmod{m} \]
Or \( (a - b)x = km \) for some integer \( k \).
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof** $\Rightarrow$ The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\Rightarrow$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m - 1\}$, where

$(ax \equiv bx \pmod m) \Rightarrow (a - b)x \equiv 0 \pmod m$

Or $(a - b)x = km$ for some integer $k$.

$\gcd(x, m) = 1$
Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of $x$ and $m$, $gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

Proof $\implies$ : The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

Pigeonhole principle: Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.
$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where

$(ax \equiv bx \mod m) \implies (a-b)x \equiv 0 \mod m$

Or $(a-b)x = km$ for some integer $k$.

$gcd(x, m) = 1$
$\implies$ Prime factorization of $m$ and $x$ do not contain common primes.
Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

Proof $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

Pigeonhole principle: Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.
$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where
$$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$$
Or $(a-b)x = km$ for some integer $k$.

$\gcd(x, m) = 1$
$\implies$ Prime factorization of $m$ and $x$ do not contain common primes.
$\implies (a-b)$ factorization contains all primes in $m$'s factorization.
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof $\implies$:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.  
$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where  
$(ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m}$  
Or $(a-b)x = km$ for some integer $k$.

$\gcd(x, m) = 1$
$\implies$ Prime factorization of $m$ and $x$ do not contain common primes.  
$\implies (a-b)$ factorization contains all primes in $m$'s factorization.  
So $(a-b)$ has to be multiple of $m$.  

Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof $\implies$:** The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m - 1\}$, where

\[(ax \equiv bx \pmod{m}) \implies (a - b)x \equiv 0 \pmod{m}
\]

Or $(a - b)x = km$ for some integer $k$.

$\gcd(x, m) = 1$

$\implies$ Prime factorization of $m$ and $x$ do not contain common primes.

$\implies (a - b)$ factorization contains all primes in $m$’s factorization.

So $(a - b)$ has to be multiple of $m$.

$\implies (a - b) \geq m$. 
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where

$(ax \equiv bx \mod m) \implies (a-b)x \equiv 0 \mod m$

Or $(a-b)x = km$ for some integer $k$.

$gcd(x, m) = 1$

$\implies$ Prime factorization of $m$ and $x$ do not contain common primes.

$\implies$ $(a-b)$ factorization contains all primes in $m$’s factorization.

So $(a-b)$ has to be multiple of $m$.

$\implies (a-b) \geq m$. But $a, b \in \{0, \ldots m-1\}$. 
Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of $x$ and $m$, $\gcd(x, m)$, is 1, then $x$ has a multiplicative inverse modulo $m$.

**Proof** $\implies$: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$.

**Pigeonhole principle:** Each of $m$ numbers in $S$ correspond to different one of $m$ equivalence classes modulo $m$.

$\implies$ One must correspond to 1 modulo $m$.

If not distinct, then $a, b \in \{0, \ldots, m-1\}$, where

$(ax \equiv bx \pmod{m}) \implies (a - b)x \equiv 0 \pmod{m}$

Or $(a - b)x = km$ for some integer $k$.

$\gcd(x, m) = 1$
$\implies$ Prime factorization of $m$ and $x$ do not contain common primes.
$\implies$ $(a - b)$ factorization contains all primes in $m$'s factorization.
So $(a - b)$ has to be multiple of $m$.

$\implies (a - b) \geq m$. But $a, b \in \{0, \ldots, m-1\}$. Contradiction.
Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of \( x \) and \( m \), \( \gcd(x,m) \), is 1, then \( x \) has a multiplicative inverse modulo \( m \).

Proof \( \implies \): The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

Pigeonhole principle: Each of \( m \) numbers in \( S \) correspond to different one of \( m \) equivalence classes modulo \( m \).
\( \implies \) One must correspond to 1 modulo \( m \).

If not distinct, then \( a, b \in \{0, \ldots, m-1\} \), where \( (ax \equiv bx \pmod{m}) \implies (a-b)x \equiv 0 \pmod{m} \)
Or \( (a-b)x = km \) for some integer \( k \).

\( \gcd(x,m) = 1 \)
\( \implies \) Prime factorization of \( m \) and \( x \) do not contain common primes.
\( \implies (a-b) \) factorization contains all primes in \( m \)'s factorization.
So \( (a-b) \) has to be multiple of \( m \).
\( \implies (a-b) \geq m \). But \( a, b \in \{0, \ldots m-1\} \). Contradiction.
Proof review. Consequence.

**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$. 
Thm: If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

Proof Sketch: The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

\( \square \)

For \( x = 4 \) and \( m = 6 \). All products of 4...
Thm: If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

Proof Sketch: The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \pmod{m} \) if all distinct modulo \( m \).

... 

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[
S = \{0, 4, 8, 12, 16, 20\} 
\]

\[
\text{reducing (mod 6)} \quad S = \{0, 4, 2, 0, 4, 2\} 
\]

Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).

\[
S = \{0, 5, 4, 3, 2, 1\} 
\]

All distinct, contains 1! 

5 is multiplicative inverse of 5 \((\text{mod 6})\).

What is \( x \)? Multiply both sides by 5.

\[
x = 15 = 3 \pmod{6} 
\]

\[
4x = 3 \pmod{6} 
\]

No solutions. Can't get an odd.

\[
4x = 2 \pmod{6} 
\]

Two solutions! \( x = 2, 5 \pmod{6} \).

Very different for elements with inverses.
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\}$
Thm: If gcd$(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing (mod 6)
Proof review. Consequence.

**Thm:** If \(\gcd(x, m) = 1\), then \(x\) has a multiplicative inverse modulo \(m\).

**Proof Sketch:** The set \(S = \{0x, 1x, \ldots, (m-1)x\}\) contains \(y \equiv 1 \mod m\) if all distinct modulo \(m\).

... For \(x = 4\) and \(m = 6\). All products of 4...

\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]

reducing \((\mod 6)\)

\[
S = \{0, 4, 2, 0, 4, 2\}
\]
**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

... 

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[ S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\} \]

reducing \( \mod 6 \)

\[ S = \{0, 4, 2, 0, 4, 2\} \]
Thm: If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

Proof Sketch: The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \pmod{m} \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]

reducing \( \pmod{6} \)

\[
S = \{0, 4, 2, 0, 4, 2\}
\]

Not distinct.
Proof review. Consequence.

**Thm:** If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

**Proof Sketch:** The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of 4...

\[ S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\} \]

reducing (mod 6)

\[ S = \{0, 4, 2, 0, 4, 2\} \]

Not distinct. Common factor 2.
Proof review. Consequence.

**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

... For \( x = 4 \) and \( m = 6 \). All products of 4...

\[ S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\} \]

reducing \( \mod 6 \)

\[ S = \{0, 4, 2, 0, 4, 2\} \]

Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).
Thm: If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

Proof Sketch: The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \pmod{m} \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]

reducing \( \pmod{6} \)

\[
S = \{0, 4, 2, 0, 4, 2\}
\]

Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).

\[
S =
\]
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... 

For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing (mod 6)

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\}$
Proof review. Consequence.

**Thm:** If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

**Proof Sketch:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing (mod 6)

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$
**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[ S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\} \]

reducing \( \mod 6 \)

\[ S = \{0, 4, 2, 0, 4, 2\} \]

Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).

\[ S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\} \]
Proof review. Consequence.

**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \pmod{m} \) if all distinct modulo \( m \).

... 

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]
reducing \( \pmod{6} \)

\[
S = \{0, 4, 2, 0, 4, 2\}
\]
Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).

\[
S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}
\]
All distinct,
Proof review. Consequence.

**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

... For \( x = 4 \) and \( m = 6 \). All products of 4...
\[ S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\} \]
reducing \( \mod 6 \)
\[ S = \{0, 4, 2, 0, 4, 2\} \]
Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).
\[ S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\} \]
All distinct, contains 1!
Proof review. Consequence.

**Thm:** If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

**Proof Sketch:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

Reducing (mod 6)

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$

All distinct, contains 1! 5 is multiplicative inverse of 5 (mod 6).
**Proof:** If \(\gcd(x, m) = 1\), then \(x\) has a multiplicative inverse modulo \(m\).

**Proof Sketch:** The set \(S = \{0x, 1x, \ldots, (m-1)x\}\) contains \(y \equiv 1 \mod m\) if all distinct modulo \(m\).

For \(x = 4\) and \(m = 6\). All products of 4...

\[ S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\} \]

reducing \(\mod 6\)

\[ S = \{0, 4, 2, 0, 4, 2\} \]

Not distinct. Common factor 2.

For \(x = 5\) and \(m = 6\).

\[ S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\} \]

All distinct, contains 1! 5 is multiplicative inverse of 5 \(\mod 6\).

\[ 5x = 3 \mod 6 \]
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

For $x = 4$ and $m = 6$. All products of $4$...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing $\pmod{6}$

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$

All distinct, contains 1! 5 is multiplicative inverse of 5 (mod 6).

$5x = 3 \pmod{6}$ What is $x$?
Thm: If \(\gcd(x, m) = 1\), then \(x\) has a multiplicative inverse modulo \(m\).

Proof Sketch: The set \(S = \{0x, 1x, \ldots, (m - 1)x\}\) contains \(y \equiv 1 \mod m\) if all distinct modulo \(m\).

For \(x = 4\) and \(m = 6\). All products of 4...
\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]
reducing \((\mod 6)\)
\[
S = \{0, 4, 2, 0, 4, 2\}
\]
Not distinct. Common factor 2.

For \(x = 5\) and \(m = 6\).
\[
S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}
\]
All distinct, contains 1! 5 is multiplicative inverse of 5 \((\mod 6)\).

\[5x = 3 \mod 6\] What is \(x\)? Multiply both sides by 5.
Proof review. Consequence.

**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...
\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]
reducing \( \mod 6 \)
\[
S = \{0, 4, 2, 0, 4, 2\}
\]
Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).
\[
S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}
\]
All distinct, contains 1! 5 is multiplicative inverse of 5 \( \mod 6 \).

\[
5x = 3 \mod 6 \quad \text{What is } x? \quad \text{Multiply both sides by 5.}
\]
\[
x = 15
\]
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing (mod 6)

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$

All distinct, contains 1! 5 is multiplicative inverse of 5 (mod 6).

$5x = 3 \mod 6$ What is $x$? Multiply both sides by 5.

$x = 15 = 3 \mod 6$
Thm: If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

Proof Sketch: The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]

Reducing \( \mod 6 \)

\[
S = \{0, 4, 2, 0, 4, 2\}
\]

Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).

\[
S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}
\]

All distinct, contains 1! 5 is multiplicative inverse of 5 \( \mod 6 \).

5\( x \equiv 3 \mod 6 \) What is \( x \)? Multiply both sides by 5.

\[
x = 15 = 3 \mod 6
\]

4\( x \equiv 3 \mod 6 \)
Proof review. Consequence.

**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...

\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]

reducing \( \mod 6 \)

\[
S = \{0, 4, 2, 0, 4, 2\}
\]

Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).

\[
S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}
\]

All distinct, contains 1! 5 is multiplicative inverse of 5 \( \mod 6 \).

\[
5x = 3 \mod 6\quad \text{What is } x? \quad \text{Multiply both sides by 5.}
\]

\[
x = 15 = 3 \mod 6
\]

\[
4x = 3 \mod 6\quad \text{No solutions.}
\]
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$.

For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing (mod 6)

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$

All distinct, contains 1! 5 is multiplicative inverse of 5 (mod 6).

$5x = 3 \pmod{6}$ What is $x$? Multiply both sides by 5.

$x = 15 = 3 \pmod{6}$

$4x = 3 \pmod{6}$ No solutions. Can’t get an odd.
Proof review. Consequence.

**Thm:** If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

**Proof Sketch:** The set $S = \{0x, 1x, \ldots, (m-1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of $4$...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing $\mod 6$

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor $2$.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$

All distinct, contains $1!$ 5 is multiplicative inverse of $5 \mod 6$.

$5x = 3 \mod 6$ What is $x$? Multiply both sides by $5$.
$x = 15 = 3 \mod 6$

$4x = 3 \mod 6$ No solutions. Can’t get an odd.
$4x = 2 \mod 6$
Proof review. Consequence.

**Thm:** If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

**Proof Sketch:** The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$.

For $x = 4$ and $m = 6$. All products of 4...

\[S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}\]

reducing $\pmod{6}$

\[S = \{0, 4, 2, 0, 4, 2\}\]

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

\[S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}\]

All distinct, contains 1! 5 is multiplicative inverse of 5 $\pmod{6}$.

$5x = 3 \pmod{6}$ What is $x$? Multiply both sides by 5.

\[x = 15 = 3 \pmod{6}\]

$4x = 3 \pmod{6}$ No solutions. Can’t get an odd.

$4x = 2 \pmod{6}$ Two solutions!
Thm: If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

Proof Sketch: The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \pmod{m}$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$ reducing (mod 6)

$S = \{0, 4, 2, 0, 4, 2\}$
Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$
All distinct, contains 1! 5 is multiplicative inverse of 5 (mod 6).

$5x = 3 \pmod{6}$ What is $x$? Multiply both sides by 5.

$x = 15 = 3 \pmod{6}$

$4x = 3 \pmod{6}$ No solutions. Can’t get an odd.

$4x = 2 \pmod{6}$ Two solutions! $x = 2, 5 \pmod{6}$
**Thm:** If $\gcd(x, m) = 1$, then $x$ has a multiplicative inverse modulo $m$.

**Proof Sketch:** The set $S = \{0x, 1x, \ldots, (m - 1)x\}$ contains $y \equiv 1 \mod m$ if all distinct modulo $m$.

... For $x = 4$ and $m = 6$. All products of 4...

$S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}$

reducing $\pmod{6}$

$S = \{0, 4, 2, 0, 4, 2\}$

Not distinct. Common factor 2.

For $x = 5$ and $m = 6$.

$S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}$

All distinct, contains 1! 5 is multiplicative inverse of 5 $(\mod 6)$.

$5x = 3 \pmod{6}$ What is $x$? Multiply both sides by 5.

$x = 15 = 3 \pmod{6}$

$4x = 3 \pmod{6}$ No solutions. Can’t get an odd.

$4x = 2 \pmod{6}$ Two solutions! $x = 2, 5 \pmod{6}$

Very different for elements with inverses.
Finding inverses.

How to find the inverse?

Algorithm:
Try all numbers up to $x$ to see if it divides both $x$ and $m$.

Very slow.

Next: A Faster algorithm.
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?
Finding inverses.

How to find the inverse?
How to find if \( x \) has an inverse modulo \( m \)?
Find \( \text{gcd} \ (x, m) \).
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?

Find $\operatorname{gcd}(x, m)$.
   Greater than 1?
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?

Find $\gcd(x, m)$.

Greater than 1? No multiplicative inverse.
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?

Find $\gcd(x, m)$.
  Greater than 1? No multiplicative inverse.
  Equal to 1?
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?

Find $\gcd(x, m)$.
  Greater than 1? No multiplicative inverse.
  Equal to 1? Multiplicative inverse.
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?

Find $\text{gcd} \ (x, m)$.
  Greater than 1? No multiplicative inverse.
  Equal to 1? Multiplicative inverse.

Algorithm:
Finding inverses.

How to find the inverse?

How to find if $x$ has an inverse modulo $m$?

Find gcd $(x, m)$.
   Greater than 1? No multiplicative inverse.
   Equal to 1? Mutliplicative inverse.

Algorithm: Try all numbers up to $x$ to see if it divides both $x$ and $m$. 
Finding inverses.

How to find the inverse?
How to find if $x$ has an inverse modulo $m$?

Find $\text{gcd} \ (x, m)$.
  Greater than 1? No multiplicative inverse.
  Equal to 1? Multiplicative inverse.

Algorithm: Try all numbers up to $x$ to see if it divides both $x$ and $m$.
Very slow.
Finding inverses.

How to find the inverse?
How to find if \( x \) has an inverse modulo \( m \)?

Find \( \gcd(x, m) \).
  Greater than 1? No multiplicative inverse.
  Equal to 1? Multiplicative inverse.

Algorithm: Try all numbers up to \( x \) to see if it divides both \( x \) and \( m \).
Very slow.

Next: A Faster algorithm.