Berkeley Math Circle
September 2022
MODULAR ARITHMETIC
Important Common Characteristics
“Addition” in Our Integer Number System

\[ \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, 3, \ldots \} \]
Important Items:

(1) Closed Within the System:
    \[
    \text{Integer} + \text{Integer} = \text{Integer}
    \]

(2) Identity \( e \):
    \[
    e + a = a + e = a
    \]

(3) Inverse \(-a\):
    \[
    a + (-a) = (-a) + a = e
    \]
Categorize this system into Groups of Special Characteristics
Even Numbers:

\{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}

(1) Even + Even = Even ?
(2) Identity ?
(3) Additive Inverses ?
Odd Numbers:

\{\ldots, -3, -1, 1, 3, 5, 7, \ldots\}

(1) Odd + Odd = Odd  
(2) Identity  
(3) Additive Inverses  
Positive Numbers:

\{1, 2, 3, 4, 5, \ldots\}

(1) Positive + Positive = Positive  ?
(2) Identity  ?
(3) Additive Inverses  ?
Positive Numbers + Zero:
\{0, 1, 2, 3, 4, 5, \ldots\}

(1) Positive + Positive = Positive ?
(2) Identity ?
(3) Additive Inverses ?
Negative Numbers + Zero:

{..., −5, −4, −3, −2, −1, 0}

(1) Negative + Negative = Negative  ?
(2) Identity  ?
(3) Additive Inverses  ?
Multiples of 3:

{..., –6, –3, 0, 3, 6, 9, ...}

(1) Multiple of 3 + Multiple of 3

= Multiple of 3 ?

(2) Identity ?

(3) Additive Inverses ?
Multiples of 10 or 23:
\{\ldots, -100, -10, 0, 10, 100, 1000, \ldots \} \\
\{\ldots, -46, -23, 0, 23, 46, 69, \ldots \} \\

(1) Multiples of 10 + Multiples of 23 = Multiples of 10 or 23 ?

(2) Identity ?

(3) Additive Inverses ?
DIVIDE AND CONQUER
Modular Arithmetic – Addition in a Finite Number System

1. Must be closed
2. Must have identity ("zero")
3. Must have additive inverse

Even = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\} \approx 0
Odd = \{\ldots, -3, -1, 1, 3, 5, 7, \ldots\} \approx 1
<table>
<thead>
<tr>
<th>+</th>
<th>Even</th>
<th>Odd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even</td>
<td>Even</td>
<td>Odd</td>
</tr>
<tr>
<td>Odd</td>
<td>Odd</td>
<td>Even</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Can view Even Numbers as multiples of 2 or divisible by 2 or remainder equals to 0 when divided by 2.

Can view Odd Numbers as the remainder of 1 when it is divided by 2.

Can view modular arithmetic as arithmetic of the remainders. We only keep track of the remainders.

Can write \( 7 \equiv 1 \pmod{2} \), \( 6 \equiv 0 \pmod{2} \)
\( 121 \equiv 1 \pmod{2} \), \( 284 \equiv 0 \pmod{2} \)
More Examples:

13 ≡ 1 (mod 3)
26 ≡ 2 (mod 3)
83 ≡ 2 (mod 3)
83 ≡ (mod 4)
83 ≡ (mod 5)
83 ≡ (mod 6)
83 ≡ (mod 9)
25675 ≡ (mod 5)
100000000000000000000 ≡ (mod 10)
25675 ≡ (mod 7)
23548901237 ≡ (mod 2)
More Examples:

\[13 \equiv 1 \pmod{3}\]
\[26 \equiv 2 \pmod{3}\]
\[83 \equiv 2 \pmod{3}\]
\[83 \equiv 3 \pmod{4}\]
\[83 \equiv 3 \pmod{5}\]
\[83 \equiv 5 \pmod{6}\]
\[83 \equiv 2 \pmod{9}\]
\[25675 \equiv 0 \pmod{5}\]
\[10000000000000000000 \equiv \pmod{10}\]
\[25675 \equiv 6 \pmod{7}\]
\[23548901237 \equiv 1 \pmod{2}\]
More Examples:

$$(\text{mod } 5) \quad 0, 1, 2, 3, \text{ and } 4 \text{ are the only remainders when an integer is divided by } 5.$$
1. 0 is the identity of \((\text{mod } 5)\)

2. 2 and 3 are additive inverses of each other since

\[2 + 3 \equiv 0 \pmod{5}\]

2 and 3 are 5-complements.

3. 4 and 1 are additive inverses of each other since

\[4 + 1 \equiv 0 \pmod{5}\]

4 and 1 are 5-complements.

4. \(-1 \equiv 4 \pmod{5}\)

5. \(-2 \equiv 3 \pmod{5}\)

6. \(-3 \equiv 2 \pmod{5}\)

7. \(-4 \equiv 1 \pmod{5}\)

8. \(5 \equiv 0 \pmod{5}\)

9. \(-72 \equiv -2 \equiv 3 \pmod{5}\)

10. \(-125 \equiv 0 \pmod{5}\)

11. \(-139 \equiv -4 \equiv 1 \pmod{5}\)
Solving equations in \((\text{mod } 5)\)

1. \(x + 3 = 12\) \hspace{1em} x = 12 + (-3) = 9 \equiv 4 \hspace{1em} (\text{mod } 5)

   Check: \hspace{1em} \text{Left Side: } x+3 = 4+3 = 7 \equiv 2 \hspace{1em} (\text{mod } 5)

   \hspace{1em} \text{Right Side: } 12 \equiv 2 \hspace{1em} (\text{mod } 5)

   Any number \(\equiv 4 \hspace{1em} (\text{mod } 5)\) works. \(124\) is a solution.

   \(124 + 3 = 127 \equiv 2 \hspace{1em} (\text{mod } 5)\)

   \(12 \equiv 2 \hspace{1em} (\text{mod } 5)\)

2. \(8x + 3 = 12–6x\) \hspace{1em} 14x = 9 \hspace{1em} 4x \equiv 4 \hspace{1em} (\text{mod } 5) \hspace{1em} x \equiv 1 \hspace{1em} (\text{mod } 5)

   Check: \hspace{1em} \text{Left Side: } 8x+3 = 8+3 = 11 \equiv 1 \hspace{1em} (\text{mod } 5)

   \hspace{1em} \text{Right Side: } 12–6x = 12–6 = 6 \equiv 1 \hspace{1em} (\text{mod } 5)

   Any number \(\equiv 1 \hspace{1em} (\text{mod } 5)\) works. \(206\) is a solution.

   \(8(206) + 3 = 1651 \equiv 1 \hspace{1em} (\text{mod } 5)\)

   \(12–6(206) = -1224 \equiv 1221 \hspace{1em} (\text{mod } 5) \equiv 1 \hspace{1em} (\text{mod } 5)\)
Applications:

Time Clock

0 to 23 (24 hours)  
18 + 23 = 41 ≡ 17 (mod 24)

0 to 12 (12 hours) with am/pm  
6 pm + 23 hours = 5 pm

15:25 vs 3:25 pm

18 + 11 pm ≡ 29 (mod 12)

≡ 5 pm

Months

January to December (1 to 12)

233 months from now (September)

233 ≡ 5 (mod 12)  
9 + 5 = 14 ≡ 2 (mod 12)  
February
Solving Equations:

\[ 9x - 7 = 5 \]
\[ 9x = 12 \quad x = 12/9 = 4/3 \quad \text{(not integer)} \]

\[ 9x - 7 \equiv 5 \pmod{12} \]
\[ 9x = 12 \equiv 0 \pmod{12} \quad x = 0 \pmod{12} \]

Check: \[ 9(0) - 7 = -7 \equiv 5 \pmod{12} \]

Any multiple of 12 works. \( x = 36. \quad 9(36) - 7 = 317 \equiv 5 \pmod{12} \)

BUT \( x = 4 \) also work. \[ 9(4) - 7 = 29 \equiv 5 \pmod{12}. \]

SO is \( x = 8. \quad 9(8) - 7 = 65 \equiv 5 \pmod{12}. \)

The real answers is any multiple of 4 and not just multiples of 12.
Consider modular multiplication

\((\text{mod } 5)\)
<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Many of the multiplication properties still hold for modular arithmetic

Identity: \( 1 \)

Commutative: \( a \times b = b \times a \)

Associative: \( a \times (b \times c) = (a \times b) \times c \)

Distributive: \( a \times (b + c) = a \times b + a \times c \)

Multiplicative Inverses: \( \frac{1}{1} = 1 \)

\( \frac{1}{2} = 3 \) \((3 \times 2 \equiv 1 \text{ (mod 5)})\)

\( \frac{1}{3} = 2 \) \((2 \times 3 \equiv 1 \text{ (mod 5)})\)

\( \frac{1}{4} = 4 \) \((4 \times 4 \equiv 1 \text{ (mod 5)})\)
Problem with Multiplication (Mod 6).

<table>
<thead>
<tr>
<th>×</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>

What are the problems?
1. Besides zero, 2, 3, and 4 have no inverses.
2. $2x \equiv 1 \pmod{6}$ has no solution.
3. $3x \equiv 1 \pmod{6}$ has no solution.
4. $4x \equiv 1 \pmod{6}$ has no solution.
5. $5x \equiv 1 \pmod{6}$ has solution $x = 5$.

What about $2x \equiv 1 \pmod{3}$, $2x \equiv 1 \pmod{4}$, $2x \equiv 1 \pmod{5}$, $2x \equiv 1 \pmod{7}$?

What about $3x \equiv 1 \pmod{2}$, $3x \equiv 1 \pmod{3}$, $3x \equiv 1 \pmod{4}$, $3x \equiv 1 \pmod{5}$, $3x \equiv 1 \pmod{7}$, $3x \equiv 1 \pmod{8}$, $3x \equiv 1 \pmod{9}$?

What about $6x \equiv 1 \pmod{15}$ or $6x \equiv 1 \pmod{17}$?
2x ≡ 1 (mod 3) \quad x = 2
2x ≡ 1 (mod 4) \quad \text{No answer}
2x ≡ 1 (mod 5) \quad x = 3
2x ≡ 1 (mod 7) \quad x = 4

3x ≡ 1 (mod 2) \quad x = 1
3x ≡ 1 (mod 3) \quad \text{No answer}
3x ≡ 1 (mod 4) \quad x = 3
3x ≡ 1 (mod 5) \quad x = 2
3x ≡ 1 (mod 7) \quad x = 5
3x ≡ 1 (mod 8) \quad x = 3
3x ≡ 1 (mod 9) \quad \text{No answer}

\textbf{What about } 6x ≡ 1 (mod 15) \text{ or } 6x ≡ 1 (mod 17)\text{?}

\text{No inverse, No answer} \quad \text{Inverse of 6 is 3, } x = 3.
Cancelling Property of Addition

14 ≡ 2 (mod 12)
14 + 2 = 16 ≡ 4 (mod 12)
2 + 2 ≡ 4 (mod 12)

Cancelling Property of Multiplication

14 ≡ 2 (mod 12)
14 × 2 = 28 ≡ 4 (mod 12)
2 × 2 = 4 ≡ 4 (mod 12)
Cancelling Property of Subtraction

\[ 14 \equiv 2 \pmod{12} \]
\[ 14 - 2 = 12 \equiv 0 \pmod{12} \]
\[ 2 - 2 \equiv 0 \pmod{12} \]

Cancelling Property of Division

\[ 14 \equiv 2 \pmod{12} \]
\[ 14 \div 2 = 7 \equiv 7 \pmod{12} \]
\[ 2 \div 2 = 1 \equiv 1 \pmod{12} \]
Cancellation Property of Multiplication

\[ a \equiv b \pmod{m} \]

\[ a - b \equiv 0 \pmod{m} \]

\[ a - b = mk \]

\[ n \times (a - b) = n \times (mk) = m(nk) \equiv 0 \pmod{m} \]

\[ na \equiv nb \pmod{m} \]
Cancellation Property of Division

\[ ac \equiv bc \pmod{m} \]

\[ ac \equiv bc \equiv 0 \pmod{m} \]

\[ ac - bc = mk \]

\[ c \times (a - b) = mk = nc \quad \text{where } n \text{ may or may not be a factor of } m \]

\[ a - b \equiv n \pmod{m} \]

but may not be \( \equiv 0 \pmod{m} \)

so \( a \) may not be \( \equiv b \pmod{m} \)
Cancellation Property of Division

$14 \equiv 2 \pmod{12}$

$14 \div 2 = 7 \equiv 7 \pmod{12}$

$2 \div 2 = 1 \equiv 1 \pmod{12}$

But

$14 \div 2 = 7 \equiv 1 \pmod{12 \div 2} \equiv 1 \pmod{6}$

So, $ac \equiv bc \pmod{m}$ implies

$a \equiv b \pmod{k}$

where $k = m/d$ with $d = \text{GCD}(m, c)$
Solving Equations

1) $3x \equiv 9 \pmod{10}$
2) $2x \equiv 4 \pmod{10}$
3) $2x \equiv 1 \pmod{3}$
4) $8x \equiv 4 \pmod{12}$
5) $6x \equiv 9 \pmod{15}$
6) $6x \equiv 2 \pmod{7}$
7) $8x \equiv 2 \pmod{12}$
8) $8x \equiv 5 \pmod{12}$
9) $8x \equiv 4 \pmod{12}$