Greatest Common Divisor:
\[ \text{GCD}(x, y) = \text{greatest } k \geq 1 \text{ s.t. } k|x \text{ and } k|y. \]

Least Common Multiple:
\[ \text{LCM}(x, y) = \text{smallest } k \geq 1 \text{ s.t. } x|k \text{ and } y|k. \]

Fact:
\[ \text{GCD}(x, y) \times \text{LCM}(x, y) = x \times y \]

Fact:
\[ (a \mod n) \text{ means the remainder when } a \text{ is divided by } n. \]
\[ a \mod n = r \iff a = dn + r \text{ for some integer } d \]
Definition: Modular equivalence

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

\[ \iff (a \mod n) = (b \mod n) \]

\[ \iff n \mid (a-b) \]

Written as \( a \equiv b \pmod{n} \) and spoken “\( a \) and \( b \) are equivalent or congruent modulo \( n \)”

\[ 31 \equiv 81 \pmod{2} \]

\[ 31 \equiv 81 \]

\[ 31 \equiv 80 \pmod{7} \]

\[ 31 \equiv 80 \]

\( n \equiv \) is an equivalence relation

In other words, it is

Reflexive: \( a \equiv a \)

Symmetric: \( (a \equiv b) \implies (b \equiv a) \)

Transitive: \( (a \equiv b \text{ and } b \equiv c) \implies (a \equiv c) \)

\( \equiv \) induces a natural partition of the integers into \( n \) “residue” classes.

(“residue” = what left over = “remainder”)

Define residue class

\([k] = \) the set of all integers that are congruent to \( k \) modulo \( n \).

Residue Classes Mod 3:

\([0] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]

\([1] = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \]

\([2] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]

\([-6] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]

\([-1] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]

Why do we care about these residue classes?

Because we can replace any member of a residue class with another member when doing addition or multiplication mod \( n \) and the answer will not change.

To calculate: \( 249 \times 504 \mod 251 \)

just do \( -2 \times 2 = -4 \equiv 247 \)

Fundamental lemma of plus and times mod \( n \):

If \( (x \equiv y) \) and \( (a \equiv b) \). Then

1) \( x + a \equiv y + b \)

2) \( x \times a \equiv y \times b \)
Proof of 2: $xa = yb \pmod{n}$
(The other proof is similar...)

Another Simple Fact:
If $(x \equiv_n y)$ and $(k|n)$, then: $x \equiv_k y$

Example: $10 \equiv_6 16 \Rightarrow 10 \equiv_3 16$

Proof:
$x \equiv_n y \Rightarrow n|(x-y)$
$k|n$
$\Rightarrow r|(x-y) \Rightarrow x \equiv_k y$

A Unique Representation System Modulo $n$:
We pick one representative from each residue class and do all our calculations using these representatives.

Unsurprisingly, we use $0, 1, 2, ..., n-1$

$\{[0], [1], [2], ..., [n-1]\}$

Unique representation system mod 3
Finite set $S = \{0, 1, 2\}$

+ and $*$ defined on $S$:

\[
\begin{array}{ccc}
+ & 0 & 1 & 2 \\
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1 \\
\end{array}
\quad
\begin{array}{ccc}
+ & 0 & 1 & 2 \\
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 \\
2 & 0 & 2 & 1 \\
\end{array}
\]

Unique representation system mod 4
Finite set $S = \{0, 1, 2, 3\}$

+ and $*$ defined on $S$:

\[
\begin{array}{ccc}
+ & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\quad
\begin{array}{ccc}
* & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

Notation
$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$

Define operations $+_n$ and $*_n$:

$a +_n b = (a + b \pmod{n})$
$a *_n b = (a * b \pmod{n})$
Some properties of the operation $+_n$

"Closed"
$x, y \in \mathbb{Z}_n \Rightarrow x +_n y \in \mathbb{Z}_n$

"Associative"
$x, y, z \in \mathbb{Z}_n \Rightarrow (x +_n y) +_n z = x +_n (y +_n z)$

"Commutative"
$x, y \in \mathbb{Z}_n \Rightarrow x +_n y = y +_n x$

Similar properties also hold for $*_n$

Unique representation system mod 3

Finite set $\mathbb{Z}_3 = \{0, 1, 2\}$

Operators defined on $\mathbb{Z}_3$

$$+_3 : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$$

$$*_3 : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$$

Finite set $Z_3 = \{0, 1, 2\}$

**Unique representation system mod 3**

Finite set $Z_3 = \{0, 1, 2\}$

two associative, commutative operators on $Z_3$

$$+_3 : Z_3 \times Z_3 \rightarrow Z_3$$

$$*_3 : Z_3 \times Z_3 \rightarrow Z_3$$

Finite set $Z_2 = \{0, 1\}$

two associative, commutative operators on $Z_2$

**Unique representation system mod 2**

Finite set $Z_2 = \{0, 1\}$

**Unique representation system mod 2**

Finite set $Z_2 = \{0, 1\}$

two associative, commutative operators on $Z_2$

$$+_2 \text{ XOR} \begin{array}{c|c|c}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}$$

$$*_2 \text{ AND} \begin{array}{c|c|c}
* & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}$$

$Z_3 = \{0, 1, 2, 3, 4\}$

$$+ \begin{array}{c|c|c|c|c}
+ & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3 \\
\end{array}$$

$$* \begin{array}{c|c|c|c|c}
* & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 \\
2 & 0 & 2 & 4 & 1 & 3 \\
3 & 0 & 3 & 1 & 4 & 2 \\
4 & 0 & 4 & 3 & 2 & 1 \\
\end{array}$$
For addition, the permutation property means you can solve, say,
\[ 4 + \_ = 1 \pmod{6} \]
\[ \_ \cdot 3 = (x \cdot 4) \pmod{6} \] for any x in \( \mathbb{Z}_6 \)

Subtraction mod n is well-defined.
Each row has a 0, hence \( -a \) is that element such that \( a + (-a) = 0 \)
\[ \Rightarrow a - b = a + (-b) \]

For multiplication, if a row has a permutation you can solve, say,
\[ 5 \cdot \_ = 4 \pmod{6} \]
or, \[ 5 \cdot \_ = 1 \pmod{6} \]

For addition, rows and columns always are a permutation of \( \mathbb{Z}_n \)

For multiplication, some rows and columns are permutation of \( \mathbb{Z}_n \), while others aren’t...

For multiplication, if a row does not have the permutation property, how do you solve
\[ 3 \cdot \_ = 4 \pmod{6} \]
\[ 3 \cdot \_ = 3 \pmod{6} \]

\[ 3 \cdot \_ = 1 \pmod{6} \] no multiplicative inverse!
Division

If you define \( 1/a \pmod{n} = a^{-1} \pmod{n} \)
as the element \( b \) in \( \mathbb{Z}_n \)
such that \( a \cdot b = 1 \pmod{n} \)

Then \( x/y \pmod{n} \) = 
\( x \cdot 1/y \pmod{n} \)
Hence we can divide out by only the \( y \)'s
for which \( 1/y \) is defined!

A visual way to understand multiplication
and the “permutation property”.

And which rows do have the permutation property?
\[
\begin{array}{cccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 \\
3 & 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 \\
4 & 0 & 4 & 8 & 12 & 16 & 20 & 24 & 28 \\
5 & 0 & 5 & 10 & 15 & 20 & 25 & 30 & 35 \\
6 & 0 & 6 & 12 & 18 & 24 & 30 & 36 & 42 \\
7 & 0 & 7 & 14 & 21 & 28 & 35 & 42 & 49 \\
\end{array}
\]

consider \( \times_8 \) on \( \mathbb{Z}_8 \)

There are exactly 8 distinct multiples of 3 modulo 8.

hit all numbers \( \iff \) row 3 has the “permutation property”

There are exactly 2 distinct multiples of 4 modulo 8.

row 4 does not have “permutation property” for \( \times_8 \) on \( \mathbb{Z}_8 \)

There are exactly 1 distinct multiples of 8 modulo 8.
There are exactly 4 distinct multiples of 6 modulo 8.

\[ \text{What's the pattern?} \]

- exactly 8 distinct multiples of 3 modulo 8.
- exactly 2 distinct multiples of 4 modulo 8.
- exactly 1 distinct multiple of 8 modulo 8.
- exactly 4 distinct multiples of 6 modulo 8.

\[ y \equiv g \left( x, \lambda \right) \mod \gamma \]

\[ \text{Theorem: There are exactly } \frac{\text{LCM}(n, c)}{c} = \frac{n}{\text{GCD}(c, n)} \text{ distinct multiples of } c \text{ modulo } n. \]

**Proof:**

Clearly, \( c/\text{GCD}(c, n) \geq 1 \) is a whole number

\[ ck = c \cdot \frac{n}{\text{GCD}(c, n)} = \frac{cn}{\text{GCD}(c, n)} \equiv 0 \]

\( \Rightarrow \) There are \( \leq k \) distinct multiples of \( c \mod n \):

\[ c \cdot 0, c \cdot 1, c \cdot 2, \ldots, c \cdot (k-1) \]

Also, \( k = \text{factors of } n \text{ missing from } c \)

\( \Rightarrow cx \equiv cy \Rightarrow n|c(x-y) \Rightarrow k(x-y) \Rightarrow x-y \geq k \)

\( \Rightarrow \) There are \( \geq k \) multiples of \( c \).

Hence exactly \( k \).

\[ \text{Theorem: There are exactly } \frac{\text{LCM}(n, c)}{c} = \frac{n}{\text{GCD}(c, n)} \text{ distinct multiples of } c \text{ modulo } n. \]

Hence, only those values of \( c \) with \( \text{GCD}(c, n) = 1 \) have \( n \) distinct multiples

(i.e., the permutation property for \( \ast_n \) on \( \mathbb{Z}_n \))

And remember, permutation property means you can divide out by \( c \) (working mod \( n \))
If you want to extend to general \( c \) and \( n \)

\[ ca \equiv_n cb \Rightarrow a \equiv_{n/\gcd(c,n)} b \]

**Fundamental lemmas mod \( n \):**

If \((x \equiv_n y)\) and \((a \equiv_n b)\). Then

1) \( x + a \equiv_n y + b \)
2) \( x \cdot a \equiv_n y \cdot b \)
3) \( x - a \equiv_n y - b \)
4) \( cx \equiv_n cy \Rightarrow a \equiv_n b \) if \( \gcd(c,n) = 1 \)

**New definition:**

\[ Z_n^* = \{ x \in Z_n \mid \gcd(x,n) = 1 \} \]

Multiplication over this set \( Z_n^* \) has the cancellation property.

**We’ve got closure**

Recall we proved that \( Z_n \) was “closed” under addition and multiplication?

What about \( Z_n^* \) under multiplication?

Fact: if \( a, b \in Z_n^* \), then \( ab \) (mod \( n \)) in \( Z_n^* \)

Proof: if \( \gcd(a,n) = \gcd(b,n) = 1 \), then \( \gcd(ab,n) = 1 \)

\[ Z_{12}^* = \{ 0 \leq x < 12 \mid \gcd(x,12) = 1 \} = \{ 1, 5, 7, 11 \} \]
Fact:
For prime \( p \), the set \( \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} \)

Proof:
It just follows from the definition!
For prim \( p \), all \( 0 < x < p \) satisfy \( \gcd(x,p) = 1 \)

\[
Z_{15}^* = \{0 \leq x < 15 \mid \gcd(x, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}
\[
\phi(12) = 4
\]

Euler Phi Function \( \phi(n) \)
\[
\phi(n) = |\text{size of } \mathbb{Z}_n^*| = |\text{number of } 1 \leq k < n \text{ that are relatively prime to } n|
\]

\[
p \text{ prime} \implies Z_p^* = \{1, 2, 3, ..., p-1\} \implies \phi(p) = p-1
\]

Theorem: if \( p, q \) distinct primes then \( \phi(pq) = (p-1)(q-1) \)

How about \( p = 3, q = 5 \)?

\[
15 - 5 - 3 + 1 = 8 = (2-1)(5-1)
\]
Theorem: if p, q distinct primes then
\[ \phi(pq) = (p-1)(q-1) \]

\[ pq = \text{# of numbers from 1 to } pq \]
\[ p = \text{# of multiples of } q \text{ up to } pq \]
\[ q = \text{# of multiples of } p \text{ up to } pq \]
\[ 1 = \text{# of multiple of both } p \text{ and } q \text{ up to } pq \]

\[ \phi(pq) = pq - p - q + 1 = (p-1)(q-1) \]

Additive inverse of a mod n
= number b such that a + b = 0 (mod n)

What is the additive inverse of a = 342952340 in \( Z_{4230493243} \)?

Answer: n – a
= 4230493243 – 342952340 = 3887540903

Multiplicative inverse of a mod n
= number b such that a * b = 1 (mod n)

How do you find multiplicative inverses fast?

Additive and Multiplicative Inverses

Remember, only defined for numbers a in \( Z_n^* \)
Theorem: given positive integers $X$, $Y$, there exist integers $r$, $s$ such that
\[ rX + sY = \gcd(X, Y) \]
and we can find these integers fast!

Now take $n$, and $a \in \mathbb{Z}_n^*$
\[ \gcd(a, n) \equiv a \mod n \]
suppose $ra + sn = 1$
then $ra \equiv 1 \mod n$
so, $r = a^{-1} \mod n$

---

**Euclid’s Algorithm for GCD**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Euclid(A,B)</td>
<td>If B=0 then return A else return Euclid(B, A mod B)</td>
</tr>
</tbody>
</table>

Euclid(67,29) \[ 67 - 2*29 = 67 \mod 29 = 9 \]
Euclid(29,9) \[ 29 - 3*9 = 29 \mod 9 = 2 \]
Euclid(9,2) \[ 9 - 4*2 = 9 \mod 2 = 1 \]
Euclid(2,1) \[ 2 - 2*1 = 2 \mod 1 = 0 \]
Euclid(1,0) outputs 1

---

**Extended Euclid Algorithm**

Let $<r,s>$ denote the number $r*67 + s*29$.
Calculate all intermediate values in this representation.

<table>
<thead>
<tr>
<th>Step</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$&lt;1,0&gt; - 2*&lt;0,1&gt; = 9$</td>
</tr>
<tr>
<td>2</td>
<td>$&lt;0,1&gt; - 3*&lt;1,2&gt; = 2$</td>
</tr>
<tr>
<td>3</td>
<td>$&lt;1,2&gt; - 4*&lt;3,7&gt; = 1$</td>
</tr>
<tr>
<td>4</td>
<td>$&lt;3,7&gt; - 2*&lt;13,30&gt; = 0$</td>
</tr>
<tr>
<td>Euclid(1,0) outputs</td>
<td>$1 = 13<em>67 - 30</em>29$</td>
</tr>
</tbody>
</table>

---

Finally, a puzzle...

You have a 5 gallon bottle, a 3 gallon bottle, and lots of water.

How can you measure out exactly 4 gallons?

---

why?

extraneous
Diophantine equations

Does the equality

$$3x + 5y = 4$$

have a solution where x, y are integers?

New bottles of water puzzle

You have a 6 gallon bottle, a 3 gallon bottle, and lots of water.

How can you measure out exactly 4 gallons?

Invariant

Suppose stage of system is given by $(L, S)$
(L gallons in larger one, S in smaller)

Set of valid moves
1. empty out either bottle
2. fill up bottle (completely) from water source
3. pour bottle into other until first one empty
4. pour bottle into other until second one full

Invariant: L, S are both multiples of 3.

Generalized bottles of water

You have a P gallon bottle, a Q gallon bottle, and lots of water.

When can you measure out exactly 1 gallon?
Recall that

if P and Q have \( \text{gcd}(P, Q) = 1 \)
then you can find integers a and b so that
\[ aP + bQ = 1 \]

Suppose a is positive, then fill out P a times
and empty out Q b times
(and move water from P to Q as needed…)

Working modulo integer \( n \)

Definitions of \( \mathbb{Z}_n \), \( \mathbb{Z}_n^* \)
and their properties

Fundamental lemmas of +, *, /
When can you divide out

Extended Euclid Algorithm
How to calculate \( c^{-1} \mod n \).

Euler phi function \( \phi(n) = |\mathbb{Z}_n^*| \)

Here’s What You Need to Know…