Number Theory and Modular Arithmetic

Greatest Common Divisor:
k = GCD(x, y)
greatest k ≥ 1 such that k|x and k|y.

Least Common Multiple:
k = LCM(x, y)
smallest k ≥ 1 such that x|k and y|k.

Fact:
GCD(x, y) × LCM(x, y) = x × y

You can use
MAX(a, b) + MIN(a, b) = a+b
to prove the above fact...

(a mod n) means the remainder
when a is divided by n.

a mod n = r
⇔
a = d n + r for some integer d
or
a = n + r k for some integer k

Definition: Modular equivalence

a = b [mod n]
⇔ (a mod n) = (b mod n)
⇔ n | (a-b)

≡n 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:

\[ [0] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]
\[ [1] = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \]
\[ [2] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]
\[ [-6] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \equiv [0] \]
\[ [7] = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \equiv [1] \]
\[ [-1] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \equiv [2] \]

\[ \equiv_n \text{ is an equivalence relation} \]
In other words, it is

Reflexive: \( a \equiv_n a \)
Symmetric: \( (a \equiv_n b) \Rightarrow (b \equiv_n a) \)
Transitive: \( (a \equiv_n b \text{ and } b \equiv_n c) \Rightarrow (a \equiv_n c) \)

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 \( -2 \times 2 = -4 = 247 \)

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

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

1) \( x + a \equiv_n y + b \)
2) \( x \times a \equiv_n y \times b \)

Proof of 2:
\( x \ a = y \ b \ (\mod \ n) \)
\[ (x \equiv_n y) \Rightarrow x = y + k \ n \]
\[ (a \equiv_n b) \Rightarrow a = b + m \ n \]
\[ x \ a = y \ b + n \ (y \ m + b \ k + k \ m) \]

Another Simple Fact:

if \( (x \equiv_n y) \) and \( (k \mid n) \), then: \( x \equiv_k y \)

Example: \( 10 \equiv_6 16 \Rightarrow 10 \equiv_3 16 \)
Proof:
\[ x = y + m \ n \]
\[ n = a \ k \]
\[ x = y + a \ m \ k \]
\[ x \equiv_k y \]
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

Unique representation system mod 2

Finite set \( Z_2 = \{0, 1\} \)

<table>
<thead>
<tr>
<th>* (_2) AND</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Unique representation system mod 3

Finite set \( S = \{0, 1, 2\} \)

+ and * defined on S:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Unique representation system mod 4

Finite set \( S = \{0, 1, 2, 3\} \)

+ and * defined on S:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Notation

\( Z_n = \{0, 1, 2, ..., n-1\} \)

Define operations \( +_n \) and \( *_n \):

\[ a +_n b = (a + b \mod n) \]

\[ a *_n b = (a * b \mod n) \]

Some properties of the operation \( +_n \)

["Closed"]

\[ x, y \in Z_n \Rightarrow x +_n y \in Z_n \]

["Associative"]

\[ x, y, z \in Z_n \Rightarrow (x +_n y) +_n z = x +_n (y +_n z) \]

["Commutative"]

\[ x, y \in Z_n \Rightarrow x +_n y = y +_n x \]

Similar properties also hold for \( *_n \)
For addition, the permutation property means you can solve, say,
\[ 4 + \_ = 1 \pmod{6} \]
\[ 4 + \_ = x \pmod{6} \]
for any \( x \) in \( \mathbb{Z}_6 \)

Subtraction mod n is well-defined

Each row has a 0,

\[ \Rightarrow a - b = a + (-b) \]

But if the row does not have the permutation property, how do you solve

\[ 3 \times \_ = 4 \pmod{6} \]
\[ 3 \times \_ = 3 \pmod{6} \]
\[ 3 \times \_ = 1 \pmod{6} \]

Division

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

Then \( x/y \pmod{n} = x \times 1/y \pmod{n} \)

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?

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</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>
<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>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>7</td>
</tr>
</tbody>
</table>

consider \(*_8\) on Z

There are exactly 8 distinct multiples of 3 modulo 8.

hit all numbers as row 3 has the “permutation property”

There are exactly 2 distinct multiples of 4 modulo 8.

row 4 does not have “permutation property” for \(*_8\) on Z

There are exactly 1 distinct multiples of 8 modulo 8.

There are exactly 4 distinct multiples of 6 modulo 8.
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
- exactly \( \frac{y}{\gcd(x,y)} \) distinct multiples of \( x \) modulo \( y \)

Theorem:

There are exactly

\[ \frac{\text{LCM}(y,x)}{x} = \frac{y}{\gcd(x,y)} \]

distinct multiples of \( x \) modulo \( y \)

Hence, only those values of \( x \) with \( \gcd(x,y) = 1 \) have \( n \) distinct multiples (i.e., the permutation property for \( \ast_n \) on \( \mathbb{Z}_n \))

Fundamental lemma of division (or cancelation) modulo \( n \):

If \( \gcd(c,n)=1 \), then \( ca \equiv_n cb \Rightarrow a \equiv_n b \)

Proof:

\[ c \cdot a \equiv_n c \cdot b \Rightarrow n \mid (ca - cb) \Rightarrow n \mid c(a-b) \]

But \( \gcd(n, c)=1 \), thus

\[ n\mid(a-b) \Rightarrow a \equiv_n b \]

If you want to extend to general \( c \) and \( n \)

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

Fundamental lemmas mod \( n \):

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

1) \( x + a \equiv_n y + b \)
2) \( x \ast a \equiv_n y \ast b \)
3) \( x - a \equiv_n y - b \)
4) \( cx \equiv_n cy \Rightarrow a \equiv_n b \)

if \( \gcd(c,n)=1 \)

New definition:

\( \mathbb{Z}_n^\ast = \{ x \in \mathbb{Z}_n \mid \gcd(x,n) = 1 \} \)

Multiplication over this set \( \mathbb{Z}_n^\ast \) has the cancellation property.
Recall we proved that $\mathbb{Z}_n$ was "closed" under addition and multiplication?

What about $\mathbb{Z}_n^*$ under multiplication?

**Fact:** if $a, b \in \mathbb{Z}_n^*$, then $a \cdot b \in \mathbb{Z}_n^*$

**Proof:** if $\gcd(a, n) = \gcd(b, n) = 1$,

then $\gcd(a \cdot b, n) = 1$

then $\gcd(a \cdot b \mod n, n) = 1$

We've got closure

For prime $p$, the set $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

**Proof:**

It just follows from the definition!

For prime $p$, all $0 < x < p$ satisfy $\gcd(x, p) = 1$

**Euler Phi Function** $\phi(n)$

$\phi(n) =$ size of $\mathbb{Z}_n^*$

= number of $1 \leq k < n$ that are relatively prime to $n$.

$p$ prime

$\Rightarrow \mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

$\Rightarrow \phi(p) = p-1$
\[ Z_{12}^* = \{0 \leq x < 12 \mid \gcd(x, 12) = 1\} = \{1, 5, 7, 11\} \]

\[ \phi(12) = 4 \]

\[ \begin{array}{c|cccc}
_1^* & 1 & 5 & 7 & 11 \\
1 & 1 & 5 & 7 & 11 \\
5 & 5 & 1 & 11 & 7 \\
7 & 7 & 11 & 1 & 5 \\
11 & 11 & 7 & 5 & 1 \\
\end{array} \]

**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 and Multiplicative Inverses**

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

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

Answer: \( n - a = 4230493243 - 342952340 = 3887540903 \)

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

Remember, only defined for numbers \( a \) in \( \mathbb{Z}_n^* \)

What is the multiplicative inverse of \( a = 342952340 \) in \( \mathbb{Z}_{4230493243} = \mathbb{Z}_n^* \)?

Answer: \( a^{-1} = 583739113 \)
How do you find multiplicative inverses fast?

**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 \( \mathbb{Z}_n^* \)
\[ \gcd(a, n) \neq 1 \implies a \in \mathbb{Z}_n^* \]
suppose \( ra + sn = 1 \)
then \( ra \equiv 1 \pmod{n} \)
so, \( r = a^{-1} \pmod{n} \)

**Extended Euclid Algorithm**

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

\[
\begin{align*}
67 &= <1,0> \\
29 &= <0,1> \\
\text{Euclid}(67,29) &= 9 = <1,0> - 2*<0,1> \\
\text{Euclid}(29,9) &= 2 = <0,1> - 3*<1,-2> \\
\text{Euclid}(9,2) &= 1 = <1,-2> - 4*<3,-7> \\
\text{Euclid}(2,1) &= 0 = <3,-7> - 2*<13,-30> \\
\text{Euclid}(1,0) \text{ outputs } 1 &= 13*67 - 30*29 \\
\end{align*}
\]

Finally, a puzzle...

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

Can you measure out exactly 4 gallons?
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?

Theorem

The linear equation
a x + b y = c
has an integer solution in x and y iff gcd(a, b) | c

=>) gcd(a, b) | a and gcd(a, b) | b => gcd(a, b) | (a x + b y)

<=) gcd(a, b) | c => c = z * gcd(a, b)

On the other hand, gcd(a, b) = x_1 a + y_1 b

z gcd(a, b) = z x_1 a + z y_1 b

c = z x_1 a + z y_1 b

Hilbert’s 10th problem

Hilbert asked for a universal method of solving all Diophantine equations
P(x_1, x_2, ..., x_n) = 0
with any number of unknowns and integer coefficients.

In 1970 Y. Matiyasevich proved that the Diophantine problem is unsolvable.

Study Bee

• Working modulo integer n
• Definitions of \( \mathbb{Z}_n \), \( \mathbb{Z}_n^* \)
• Fundamental lemmas of +, -, *, /
• Extended Euclid Algorithm
• Euler phi function \( \phi(n) = |\mathbb{Z}_n^*| \)