Modular World

Defn. Let m be a positive integer (called a modulus).

Say two integers a and b are congruent modulo m, written as

$$a \equiv b \mod m$$

if $m \mid a-b$

Defn. Let x be an integer and m a modulus.

The natural representation of x modulo m is the remainder r left under the division algorithm

$$x = q \cdot m + r, \quad 0 \leq r < m.$$

Note that $x \equiv r \mod m$.

Prop. Two integers a and b are congruent modulo m if and only if they have the same natural representation modulo m.

Prop. Let m be a modulus, and a, b, c, d are integers s.t.

$$a \equiv b \mod m \quad \& \quad c \equiv d \mod m$$

Then $a+c \equiv b+d \mod m$ & $ac \equiv bd \mod m$

(E.g.) Find the natural representation of $2^{10} \mod 7$

$$2^{10} = 2^3 \cdot 2^3 \cdot 2^3 \cdot 2 \equiv 1 \cdot 1 \cdot 1 \cdot 2 \equiv 2 \mod 7.$$

Since $2^3 = 8 \equiv 1 \mod 7$

Note that $10 \equiv 3 \mod 7$, but $2^{10} \not\equiv 2^3 \mod 7$.

Namely: in general $a^c \not\equiv b^d \mod m$.

Prop. ("congruent modulo m" is an equivalence relation)

i) reflexity : $a \equiv a \mod m$ for all $a \in \mathbb{Z}$

ii) symmetricity : "$a \equiv b \mod m$" $\Longleftrightarrow$ "$b \equiv a \mod m$".

iii) transitivity : "$a \equiv b \mod m$" and "$b \equiv c \mod m$"
$\Rightarrow$ "$a \equiv c \mod m$".

Outputs:

$X \quad \sim$

$\Rightarrow [a] := \{ x \in X : a \sim x \}$

- equivalent class $[a]_m$ of $a \in \mathbb{Z}$:

  it is the set of all integers congruent to a modulo m

  Other notation: $[a]$ or $\bar{a}$ (If the modulus m is clear)

e.g. $[3]_5 = \{ 3 + 5 \cdot n \mid n \in \mathbb{Z} \}$, $[0]_2 = \{$even integers$\}$, $[1]_2 = \{$odds$\}$

- It makes sense to define & consider the quotient set

$$\mathbb{Z}/m := \{ [a]_m \mid a \in \mathbb{Z} \}. \quad \left(\mathbb{Z}/m\mathbb{Z} \;,\; \cancel{\mathbb{Z}_m} \right)$$

"congruence modulo m"

from Abstract Algebra

But many of them are the same:

Indeed, $[a]_m = [b]_m \iff a \equiv b \mod m$.

$$\rightsquigarrow \quad \mathbb{Z}/m = \{ [0]_m, [1]_m, \cdots, [m-1]_m \}$$

$\sim \updownarrow$ "natural representation modulo m"

$$\{ 0, 1, \cdots, m-1 \}$$

Outputs:

Addition & multiplication of equivalent classes:

- $$[a]_m + [b]_m = [a+b]_m$$

$$\left\{ x+y \;\middle|\; \begin{matrix} x \equiv a \bmod m \\ y \equiv b \bmod m \end{matrix} \right\} = \left\{ z \;\middle|\; z \equiv a+b \bmod m \right\}$$

- $$[a]_m \cdot [b]_m = [a \cdot b]_m$$

$$\left\{ x \cdot y \;\middle|\; \begin{matrix} x \equiv a \bmod m \\ y \equiv b \bmod m \end{matrix} \right\} = \left\{ z \;\middle|\; z \equiv a \cdot b \bmod m \right\}$$

We have a <u>ring</u> $(\mathbb{Z}/m, +, \cdot, [0]_m, [1]_m)$

$[a]_m + [0]_m = [a]_m$

Similar to $(\mathbb{Z}, +, \cdot, 0, 1)$

$[a]_m \cdot [1]_m = [a]_m$

Whenever one has a ring R (e.g. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$),

and $a, b \in R$, say say a divides b in R means

the linear equation $ax = b$ has a solution in R.

For example: 2 divides 3 in $\mathbb{Q}$ but not in $\mathbb{Z}$.

$2x = 3$

Say an element $a \in R$ is a unit if a divides 1.

the identity element

$(\forall x \in R,\ x \cdot 1 = 1 \cdot x = x)$

e.g. The only units in $\mathbb{Z}$ are ± 1.

All nonzero elements in $\mathbb{Q}$ (and in $\mathbb{R}$, $\mathbb{C}$) are units.

If $a \in R$ is a unit, then the only solution of $ax = 1$

in R is called the multiplicative inverse of a. (Notation: a^{-1}).

Division in $\mathbb{Z}/m$.

Defn. Let m be a modulus, and a an integer.
Say $b \in \mathbb{Z}$ is a multiplicative inverse of a modulo m if

$$a \cdot b \equiv 1 \mod m.$$

Note that, this implies $\overline{a} \cdot \overline{b} = \overline{1}$

e.g. $2 \cdot 3 \equiv 1 \mod 5$, $2 \cdot 4 \equiv 1 \mod 7$.

When a has a multiplicative inverse modulo m, we say a is invertible modulo m.

(i.e. $[a]_m$ is a unit in $\mathbb{Z}/m$)

Thm. Let m be a modulus, and a an integer.

(1) a is invertible modulo m if and only if $GCD(a,m)=1$.
($\bar{a}$ is a unit in $\mathbb{Z}/m$)

(2) If a is invertible modulo m, then any multiplicative inverses of a modulo m are congruence to each other modulo m.

Proof: (1) " a is invertible modulo m "

$$\Updownarrow$$

" $\exists b \in \mathbb{Z} : ab \equiv 1 \bmod m$ "

$$\Updownarrow$$

" $\exists b \in \mathbb{Z} : m \mid ab - 1$ "

$$\Updownarrow$$

" $\exists b \in \mathbb{Z} : \exists x \in \mathbb{Z} : ab - 1 = xm$ " $ab - mx = 1$

$$\Updownarrow$$

" $GCD(a,m) = 1$ "

(2) Suppose b & b' are two multiplicative inverse of a modulo m then

$$b = b \cdot 1 \equiv b \cdot (a b') \equiv (b \cdot a) \cdot b' \equiv 1 \cdot b' = b' \mod m$$

Coro. (CANCELING)

- If a is invertible modulo m, then

$2 \cdot 1 \equiv 2 \cdot 3 \mod 4$
But $1 \not\equiv 3 \mod 4$

$$ax \equiv ay \mod m \quad \Rightarrow \quad x \equiv y \mod m$$

- If a is invertible modulo m, then

$$ax \equiv c \mod m$$

has solutions :

$$x \equiv a^{-1} c \mod m$$

$[a]_m \cdot X = [c]_m$

$\Updownarrow$

$X = [a^{-1} c]_m$

Example:

Solve : $15x \equiv 4 \mod 37$

1) $GCD(15, 37) = ?\ 1$

$$37 = 2 \cdot 15 + 7$$
$$15 = 2 \cdot 7 + 1$$
$$7 = 7 \cdot 1 + 0$$

$$1 = 15 - 2 \cdot 7$$
$$= 15 - 2 \cdot (37 - 2 \cdot 15)$$
$$= 5 \cdot 15 - 2 \cdot 37$$

2) Find a multiplicative inverse of 15 mod 37.

5 is a multiplicative inverse of 15 mod 37

3) Canceling: $15x \equiv 4 \mod 37$

multiply both side by the multiplicative inverse.

$$\Leftrightarrow x \equiv 5 \cdot 4 = 20 \mod 37$$

Modular Dynamics

Given a set X and a function $f: X \to X$, the dynamics of f means the sequences $x_0, f(x_0), f(f(x_0)), \cdots, f^n(x_0), \cdots$ where $x_0 \in X$.

$$X \xrightarrow{f} X \xrightarrow{f} X \longrightarrow \cdots$$

e.g. Consider $X = \mathbb{N}$ and $f: \mathbb{N} \to \mathbb{N}$ given by

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even.} \\ 3n+1 & \text{if } n \text{ is odd.} \end{cases}$$

Say $x_0 = 17$. Then the dynamic of f starting from 17 is

$$17 \longrightarrow 52 \longrightarrow 26 \longrightarrow 13 \longrightarrow 40 \longrightarrow 20 \longrightarrow 10 \longrightarrow 5$$

$$\longrightarrow 16 \longrightarrow 8 \longrightarrow 4 \longrightarrow 2 \longrightarrow 1$$

Conjecture (Collatz, 3N+1)

In the above dynamic, for any $x_0 \in \mathbb{N}$, the dynamic stops at 1 after n step for some $n > 0$. (i.e. $f^n(x_0) = 1$)

Still open, so dynamic problem could be difficult!

Modular Dynamic focus on subsets of $\mathbb{Z}/m$.

- (Additive Modular Dynamic)

Let m be a modulus, and a an integer. Consider

$$\boxed{+a \bmod m} : \mathbb{Z}/m \longrightarrow \mathbb{Z}/m$$
$$\overline{x} \longmapsto \overline{x+a}$$

e.g. $X = \mathbb{Z}/_{21}$, $a = 6$

$$\begin{tikzcd}
\overline{0} \arrow[r] \arrow[d, equal] & \overline{6} \arrow[r] & \overline{12} \arrow[r] & \overline{18} \arrow[r] & \overline{24} \arrow[dl, equal] \\
\overline{21} & \overline{15} \arrow[l] & \overline{9} \arrow[l] & \overline{3} \arrow[l] & \\
\overline{1} \arrow[r] \arrow[d, equal] & \overline{7} \arrow[r] & \overline{13} \arrow[r] & \overline{19} \arrow[r] & \overline{25} \arrow[dl, equal] \\
\overline{22} & \overline{16} \arrow[l] & \overline{10} \arrow[l] & \overline{4} \arrow[l] & \\
\overline{2} \arrow[r] \arrow[d, equal] & \overline{8} \arrow[r] & \overline{14} \arrow[r] & \overline{20} \arrow[r] & \overline{26} \arrow[dl, equal] \\
\overline{23} & \overline{17} \arrow[l] & \overline{11} \arrow[l] & \overline{5} \arrow[l] &
\end{tikzcd}$$