Modular Arithmetic (12.1)

Definition Let $x, y \in \mathbb{Z}$ & $m \in \mathbb{N}$. Then x is congruent to y modulo m if $x-y$ is divisible by m.

Write $x \equiv_m y$ or $x \equiv y \mod m$.

Ex $0 \equiv 2 \equiv 4 \equiv -2 \equiv \cdots \mod 2$

$1 \equiv 3 \equiv 5 \equiv \cdots \mod 2$

$2 \equiv 12 \mod 5$, since $12-2=10$ is divisible by 5.

Ex Say 1 March is a Monday, then $1 \equiv 8 \equiv 15 \equiv 22 \equiv 29 \mod 7$ shows 8 March, 15 March etc. are Mondays.

Remark $\equiv_m$ is equivalence relation on $\mathbb{Z}$

(1) $x \equiv x \mod m \quad \forall x \in \mathbb{Z}$

(2) $x \equiv y \mod m \iff y \equiv x \mod m \quad \forall x, y \in \mathbb{Z}$

(3) $x \equiv y$ & $y \equiv z \implies x \equiv z$

For $x \in \mathbb{Z}$, the congruence class of x mod m is

$$[x]_m = \{ y \in \mathbb{Z} \mid y \equiv x \mod m \} = \{ x + km \mid k \in \mathbb{Z} \}$$

Ex $[0]_3 = \{ \ldots, -3, 0, 3, 6, \ldots \} = [3]_3 = [6]_3 = \cdots$

$[1]_3 = \{ \ldots, -2, 1, 4, 7, \ldots \}$

$[2]_3 = \{ \ldots, -1, 2, 5, 8, \ldots \}$

Every $x \in \mathbb{Z}$ is congruent to one of $0, 1, 2, \ldots, m-1 \mod m$.

A complete set of congruence classes mod m is

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$

The ring of integers modulo m or residue class ring is

$$\mathbb{Z}_m = \{ [0], [1], \ldots, [m-1] \}.$$

"Ring" means this set has operation of addition & multiplication

$$[x]+[y]=[x+y] \qquad x,y \in \mathbb{Z}$$
$$[x][y]=[xy]$$

satisfying "usual rules" of arithmetic

- $[0]+[x]=[x]$
- $[1][x]=[x]$
- $([x]+[y])+[z]=[x]+([y]+[z])$

etc.

Addition tables: $m=4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$m=5$

+	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

·	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

E.g. $3\cdot 4 = 12 \equiv 2 \mod 5$, $4\cdot 4 \equiv 16 \equiv 1 \mod 5$

Example Divisibility checks: Let $n = a_s a_{s-1} \cdots a_0$ be the decimal representation of an integer, let $m \in \mathbb{N}$. Since $n = a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_0$,

n is divisible by $m \iff \sum_{i=0}^{s} a_i 10^i \equiv 0 \mod m$.

- $m=10$, $a_0 + a_1\cdot 10 + a_2 \cdot 10^2 + \cdots + a_s \cdot 10^s \equiv a_0 \mod 10$,
  so n divisible by $10 \iff a_0 = 0$.
- $m=9$ $a_0 + a_1 \cdot 10 + \cdots + a_s 10^s \equiv a_0 + a_1 + \cdots + a_s \mod 9$,
  n divisible by $9 \iff$ digit sum divisible by 9 (126)
- $m=11$ $a_0 + a_1 \cdot 10 + \cdots + a_s 10^s \equiv a_0 + a_1\cdot(-1) + a_2\cdot(-1)^2 + \cdots$
  $= a_0 - a_1 + a_2 - a_3 - \cdots + (-1)^s a_s \mod 11$.

n divisible

Ex 1 2 2 3 2 is divisible by 11, since $2-3+2-2+1=0$.

Structure of $\mathbb{Z}_m$

$m \in \mathbb{N}$

Given $a, b, c \in \mathbb{Z}$, could want to solve (congruence) equation

$$ax + b \equiv c \pmod{m},$$ i.e. find what x is mod m.

Proceeding in usual way, this is equivalent to

$$ax \equiv c - b \pmod{m},$$

but now we are in trouble, since we can not divide by a.

Ex Looking at examples, from the multiplication tables, can have 0, 1 or many solutions:

$2x \equiv 3 \pmod 5 \iff x \equiv 4 \pmod 5$

$2x \equiv 1 \pmod 4$ impossible

$2x \equiv 0 \pmod 4 \iff x \equiv 1$ or $x \equiv 3 \pmod 4$

Def We say $\mathbb{Z}_m$ is a field if for every $x \neq [0]$ in $\mathbb{Z}_m$, there is a y such that $xy = 1$ in $\mathbb{Z}_m$.

Ex $\mathbb{Z}_5$ is a field

x	y
1	1
2	3
3	2
4	4

, $\mathbb{Z}_4$ is not a field, since no solution to $2y \equiv 1 \pmod 4$.

Rmk If $xy = 1$ in $\mathbb{Z}_m$, then y is uniquely determined by x: Given two y_1, y_2 s.t. $y_1 x = 1$ & $y_2 x = 1$, find

$$y_2 = 1 y_2 = y_1 x y_2 = y_1 1 = y_1.$$

Write $y = x^{-1}$ or $y = \frac{1}{x}$.

Thm Let $m \geq 2$. Then the following are equivalent

a) m is prime

b) $\mathbb{Z}_m$ is a field.

Pf a) $\Rightarrow$ b) **Claim**: Let m be prime, let $x, y \in \mathbb{Z}_m$, $x, y \neq 0$. Then $xy \neq 0$ in $\mathbb{Z}_m$.

Pf of claim: Represent x, y by integers $\bar{x}, \bar{y}$. These have prime factorisation

$$\bar{x} = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \qquad \bar{y} = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n},$$

where $p \neq p_i$ for all i (since $\bar{x}, \bar{y} \not\equiv 0 \pmod{p}$).

Since $\bar{x}\bar{y} = p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_n^{e_n+f_n}$, it follows $\bar{x}\bar{y} \not\equiv 0 \pmod{p}$, so $xy \neq 0$.

Let now $x \in \mathbb{Z}_m$, $x \neq 0$, and assume m prime. Consider the function

$$f : \mathbb{Z}_m \to \mathbb{Z}_m \qquad f(y) = xy.$$

This is injective, since

$$f(y_1) = f(y_2) \iff xy_1 = xy_2 \iff x(y_1 - y_2) = 0 \overset{x \neq 0}{\iff} y_1 - y_2 = 0 \iff y_1 = y_2.$$

But then it is surjective, so find y s.t. $f(y) = 1$.

b) $\Rightarrow$ a) If m is not prime, write $m = ab$, $1 < a, b < m$. Have $a, b \neq 0$ in $\mathbb{Z}_m$, but $ab = 0$. If y is s.t. $ay = 1$, then $b = bay = 0y = 0$, which is absurd. Hence there is no y s.t. $ay = 1$.

Cor If p is prime, $a, b, c \in \mathbb{Z}_p$, $a \neq 0$, then $ax + b = c$ has unique solution in $\mathbb{Z}_p$.

Pf Take $x = (c - b)a^{-1}$.

Fermat's theorem Let p be prime, $a \in \mathbb{Z}$ not divisible by p. Then $a^{p-1} - 1$ is divisible by p.

Pf Equivalent to $a \in \mathbb{Z}_p$ $a \neq 0 \Rightarrow a^{p-1} - 1 = 0 \iff a^{p-1} = 1$.

Since $f : \mathbb{Z}_p \to \mathbb{Z}_p$ $f(y) = ay$ is bijective, have

$\{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, \ldots, p-1\}$.

So

$a(2a)(3a)\cdots(p-1)a = 1 \cdot 2 \cdot 3 \cdot \cdots (p-1)$ in $\mathbb{Z}_p$.

$\Downarrow$ p is prime, so division allowed!

$a\,a\,a \cdots a\,(p-1)! = (p-1)!$

$\Downarrow$

$a^{p-1} = 1$.

□